



**Final Report**  
of the  
**Year 2000**  
**Y2K**  
**International Security Dimension Project**

**Dr. Thomas P.M. Barnett**

*with*

**Prof. Henry D. Kamradt**

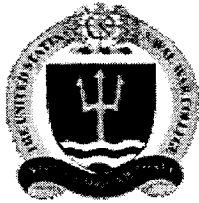
*and based on inputs from*

**Dr. Lawrence Modisett**  
**Prof. Bradd C. Hayes**  
**Prof. Theophilos C. Gemelas**  
**Prof. Gregory Hoffman**

*Originally posted 23 July 1999 at <http://www.nwc.navy.mil/y2k>*



**Report Number 00-5**



U.S. Naval War College

## Year 2000 International Security Dimension Project Final Report

Dr. Thomas P.M. Barnett

*with*

Prof. Henry D. Kamradt

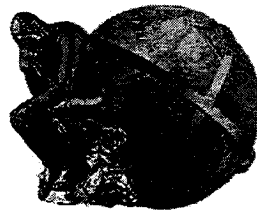
*and based on inputs from*

Dr. Lawrence Modisett

Prof. Bradd C. Hayes

Prof. Theophilos C. Gemelas

Prof. Gregory Hoffman



**Decision Strategies Department**

*Originally posted 23 July 1999 at <http://www.nwc.navy.mil/y2k>*



Please contact Dr. Thomas P.M. Barnett (401.841.4053 or [barnettt@nwc.navy.mil](mailto:barnettt@nwc.navy.mil))  
for any further information on the study or to provide feedback on this report

## **TABLE OF CONTENTS**

<b>I.</b>	<b>Introduction</b>	<b>Page 1</b>
<b>II.</b>	<b>Our Big Picture Approach</b>	<b>Page 9</b>
<b>III.</b>	<b>A Series of Y2K Onset Models</b>	<b>Page 19</b>
<b>IV.</b>	<b>The M Curve of Influence</b>	<b>Page 37</b>
<b>V.</b>	<b>The Scenario Dynamics Grid</b>	<b>Page 47</b>
<b>VI.</b>	<b>Some Preliminary Thinking on CINCs' Strategies</b>	<b>Page 71</b>
<b>VII.</b>	<b>A View From Wall Street</b>	<b>Page 85</b>
<b>VIII.</b>	<b>Some Cosmic Conclusions About Y2K</b>	<b>Page 101</b>
	<b>Appendix: List of Workshop Participants</b>	<b>Page 107</b>

# I. Introduction

## How This Project Started and Why

The Year 2000 International Security Dimension Project is the brainchild of Vice Admiral Arthur K. Cebrowski, President of the U.S. Naval War College. For those familiar with his career, this should come as no surprise, as he has long served as a leading thinker within the military regarding the intersection of technology and global change. Admiral Cebrowski believes the Year 2000 Problem (hereafter Y2K) can have a significant historical impact on humanity's relationship with technology, if only to rapidly teach us all a great deal about what it means to live in an increasingly interdependent, interconnected, and information technology-driven globalized economy.

Soon after assuming his post at the War College in the summer of 1998, Admiral Cebrowski tasked the Center for Naval Warfare Studies' Decision Strategies Department, led by Dr. Lawrence Modisett, to engage in a year-long study of Y2K's potential to trigger significant scenarios of internal or transnational instability in the world outside the United States. We've since defined "significant scenarios" to mean a crisis situation of sufficient magnitude to demand—under the potentially unprecedented global circumstances of Y2K—Department of Defense (DoD) attention in terms of possible crisis response. Such a response could range from anything as minor as the rapid insertion of a small "tiger team" to help foreign nationals repair a specific network facility, to something on the order of a Complex Humanitarian Emergency mission to some country or region especially hard hit. In short, it's a wide-open playing field, with a key uncertainty being how the United States itself weathers the Y2K Event.

From the beginning of this project, we've stressed an "agnostic" approach on Y2K and its potential impact, meaning we seek neither to rally a broad social or governmental response to deal with this problem (e.g., the ongoing remediation effort) nor to present any sort of "official" government outlook on what is likely to happen. Instead, we've approached the Y2K event as we would any other potentially destabilizing event of serious political-military impact—by employing a standard decision scenario approach. By "decision scenario approach," we mean using credible scenarios to create awareness among relevant decision-makers regarding the sort of strategic issues and choices they are likely to face if the more stressing pathways envisioned come to pass. Naturally, because we work for the military, we're more interested in the "darker" scenarios. That doesn't mean we expect or predict really bad things will happen, only that we think it's essential the U.S. Military must consider the potential scope of the problem in advance so as to avoid both errors of omission and commission once the Y2K Event begins—with an emphasis on the latter.



## How We View the "Whole Enchilada"

As you'll notice, we call our project the *Year 2000* International Security Dimension Project—not the *Y2K* International Security Dimension Project. Why? It's our firm contention that DoD should view the Millennial Date Change Event as comprising a constellation of simultaneously unfolding elements, of which Y2K is clearly the most important. Our draft list of globally significant pieces to this puzzle would begin as follows:

- Year 2000 computer problem (e.g., software and embedded chips) in and of itself
- Y2K—the global remediation effort and all that it entails
- Y2K as a global education process regarding the pervasiveness of "all this invisible technology"
- Y2K as a global crisis management challenge and economic threat
- Global economy just coming off a period of significant widespread turmoil (e.g., the Asian Financial Crisis of 1997 and its subsequent spread to Russia and Brazil), resulting in significant reform efforts by many of the affected countries
- Millennial Event in its largely secular form, i.e., the "world's largest party ever"
- Millennial Event in its religious form, i.e., celebrating the onset of the Third Millennium since Christ's birth
- Millennial Event in its socio-political form, i.e., marking a milestone period in the planet's history during which political leaders, as well as ordinary citizens, engage in extraordinary debate regarding the status quo and what should logically follow
- Millennial Event in its extremist form, i.e., the strong assumption by some in society that the event will usher in profound and cataclysmic global change, typically associated with apocalyptic visions involving a deity or supernatural force
- Tendency of humans to seek grand unifying theories for periods of history that involve above-average levels of complexity, and utilize those theories as guides for self-perceived "strategic" action.

Looking at that list, you quickly come to the conclusion, as we did last fall, that this was not a subject one could handle in the typical BOGGSAT-style (Bunch Of Guys & Gals Sitting Around a Table). No, we needed *many* bunches of guys and gals sitting around *many* tables, parsing out this huge puzzle from a variety of perspectives. Since the Deci-

sion Strategies Department's greatest expertise comes in talking with experts and synthesizing their views for wider distribution, we soon settled on a workshop approach that would involve a very broad range of expertise outside the military. [A complete list of our workshop participants can be found in the Appendix.]

Looking over that list, we likewise came to the conclusion that, since the Millennial Date Change Event appears to have so much "baggage" and "fellow travelers," so to speak, our project risked expanding into a study about *anything happening to anyone anywhere in the world come 1 January 2000*. While not shying from that challenge, for you'll see that comprehensiveness is our calling card, we readily realized that ours would not be a technical approach of lists upon lists of things that could go wrong. Rather, we decided that the most feasible approach for a small research unit such as ours would be to concentrate on the broad dynamics of the possible scenarios, to include not only the functioning of networks (broadly defined as any distributed system that moves material), but economic activity, societal responses, as well as the operations of government entities.

In a nutshell, then, our project became focused—despite the broad nature of the subject matter—on the possible scenario dynamics the Defense Department could face if it were tasked by the national leadership to engage in crisis response activities abroad during the Millennial Date Change Event and the subsequent unfolding of the Y2K Event. Mind you, our assumption going in was that we would not uncover any new or unprecedented missions for the CINCs (Commanders in Chief) of DoD's various regional military commands (e.g., Southern Command covering Latin America, Central Command covering Southwest Asia, European Command covering Europe and most of Africa, and Pacific Command covering most of Asia in addition to the Pacific island states)—and, to date, we have not found any. Rather, our assumption has been all along that, while the CINCs are likely to engage in very familiar missions of crisis response, it is the *internal* or *regional dynamics* into which they may delve that will be unusual and worth preparing for in advance.

## The Structure and Schedule of the Workshops

We conducted four workshops, starting in December 1998 and concluding in May 1999.

### DECEMBER SCENARIO-BUILDING WORKSHOP

For our first workshop in December of 1998, we invited about two dozen subject-matter experts to help us construct and flesh out a series of generic onset models (presented later). The experts invited fell into four rough categories of knowledge and experience:

- Distribution/Service Networks (e.g., food, basic needs, oil/gasoline, air and mass transit, electric power, and telecom service)

- Business activity (e.g., major manufacturing, major retail, medical, insurance, and finance-banking)
- Social communications (e.g., mass media, government regulation of mass media, face-to-face and individual comms, the Internet)
- Government services (e.g., defense, police, basic services, and emergency services).

Visit our archive web site (<http://www.nwc.navy.mil/y2k>) to view the read-ahead package for the December Scenario-Building workshop held at the Decision Support Center of Sims Hall at the U.S. Naval War College in Newport, RI.

The participants at this event provided us with a number of useful and imaginative inputs via a meeting facilitation software program known as GroupSystems (e.g., scenario pieces presented in the format of "newspaper headlines," possible warning indicators of events moving from one scenario to another, "bumper sticker" names for individual scenarios), in addition to their moderated participation in nine separate discussion sessions covering the following topics:

- Y2K as a series of discrete and periodic events
- Y2K as a widespread and sustained event
- What makes a country's "networks" (broadly defined to include social networks) robust?
- What makes them vulnerable?
- Signposts indicating the nature of the Y2K event's unfolding
- The best-case scenario (Y2K as discrete/periodic and systems are robust)
- The next-best-case scenario (Y2K as sustained/widespread and systems are robust)
- The next-worst-case scenario (Y2K as discrete/periodic and systems are vulnerable)
- The worst-case scenario (Y2K as sustained/widespread and systems are vulnerable)
- "You Make the Call!" on Y2K both within the U.S. and around the world.

We were able to gather and edit several hundred ideas and scenario vignettes from the various GroupSystems sessions and subsequently published them on our web site at the Naval War College. Visit our archive web site (<http://www.nwc.navy.mil/y2k>) to view the GroupSystems inputs from this workshop.

## JANUARY SCENARIO-DYNAMICS WORKSHOP

At our second workshop in January of 1999, we brought together about two dozen subject-matter experts with a strong experience/knowledge base in networks, business activity, social issues and/or government in one of five world regions:

- Western Hemisphere outside of U.S.
- Europe (to include Russia)
- Southwest Asia (to include Middle East, Central Asia, and Indian sub-continent)
- Asia
- Africa.

Visit our archive web site (<http://www.nwc.navy.mil/y2k>) to view the read-ahead package for the January Scenario-Dynamics workshop held at the Senator Claiborne Pell Center of Salve Regina University in Newport, RI.

Participants at this event provided the study team with a number of useful and imaginative inputs via the GroupSystems approach (e.g., advice-filled "e-mails" written to their "close personal friend" who serves as top policy adviser to the President of Country X), in addition to their moderated participation in eight separate discussion sessions covering the following topics:

- "Mania" phase of the Y2K event (see the section, *The M Curve of Influence* for details)
- "Countdown" phase
- "Onset" phase
- "Unfolding" phase
- "Peak" phase
- "Exit" phase
- Possible malevolent acts by those seeking to destabilize social order
- Region-by-region predictions as to how Y2K will impact nation-states.

We were able to gather and edit several hundred ideas and scenario vignettes from the various GroupSystems sessions and subsequently published them on our web site. Visit our archive web site (<http://www.nwc.navy.mil/y2k>) to view the GroupSystems inputs from this workshop.

## **MARCH SCENARIO-STRATEGIES WORKSHOP**

At our third workshop in March 1999, we explored the possible range of DoD policy measures and associated CINC regional strategies that might be pursued in response to the unfolding of the Y2K and associated Millennial Date Change Events, along the phased scenario timeline developed and populated in the January workshop. While we benefited by some CINC representation, our real focus was on tapping into the extant inside-the-Beltway knowledge base regarding Y2K contingency planning, with an eye toward blending that knowledge with our own for eventual provision to the individual CINCs as both they and the Joint Staff begin planning against the threat of Y2K-induced crises around the world. The participants at this workshop came mainly from defense-related federal agencies and think tanks.

Visit our archive web site (<http://www.nwc.navy.mil/y2k>) to view the read-ahead package for the March Scenario-Strategies workshop held at the headquarters of The CNA Corporation in Alexandria, VA.

Participants at this event provided the study team with a number of interesting and illuminating inputs via the GroupSystems approach, which in this instance involved providing us feedback on our proposed list of "policy do's and don'ts" for the governing authorities of a notional country as well, as our list of possible CINC mission categories (see the read-ahead package for details). For purposes of the one-day workshop, we reduced our six-phase scenario timeline to the following three groupings (which formed the basis for our three discussion sections):

- "Mania/Countdown" phases
- "Onset/Unfolding" phases
- "Peak/Exit" phases.

We were able to gather and edit several dozen ideas and commentaries from the various GroupSystems sessions and subsequently published them on our web site. Visit our archive web site (<http://www.nwc.navy.mil/y2k>) to view the GroupSystems inputs from this workshop.

## **MAY ECONOMIC SECURITY WORKSHOP**

At our fourth and final workshop in May 1999, we focused on how global financial markets would "process" and/or be impacted by the Y2K event. Most specifically, we were interested in exploring how Y2K could trigger a "new rule set" for the international economy by further crystallizing some of the most pressing issues arising from the Global Fi-

nancial Crisis of 1997-98 (e.g., push for more controls over international capital flows, calls to revamp/reform the IMF, more transparency in Emerging Markets and Hedge Funds, *de facto* dollarization of some economies). The participants at this workshop came from a variety of Wall Street investment banks, brokerage firms, and related financial organizations.

Visit our archive web site (<http://www.nwc.navy.mil/y2k>) to view the read-ahead package for the May Economic Security workshop hosted by Cantor Fitzgerald LP in the World Trade Center in Manhattan, New York.

Participants at this event provided the study team with a number of interesting and illuminating inputs via the GroupSystems approach, which in this instance involved providing us with arguments—both pro and con—as to Y2K's potentially negative impact—both short and long term—on global financial markets across the same three scenario-phase pairings employed in the March workshop.

We were able to gather and edit several dozen ideas and commentaries from the various GroupSystems sessions and subsequently published them on our web site. Visit our archive web site (<http://www.nwc.navy.mil/y2k>) to view the GroupSystems inputs from this workshop.

## Some Caveats Before Proceeding

Understanding that there is a tremendous gap between the public face many corporations and governments put forward on this issue ("we will have it well in hand") and the private fears and concerns expressed by many information technology experts (ranging from "global recession" to "apocalypse 2000!"), we wanted to explore this topic in as systematic a fashion as possible. We've never pretended that we'll end up with all the answers, but merely a sensible read on what's possible, how governments and companies are likely to respond across a range of scenarios, and what the USG and DoD should be prepared to undertake in response to Y2K's global unfolding. In short, while we're not interested in unduly hyping the Y2K situation, we are interested in exploring the "dark side" potentials because, frankly, that's what we get paid to do as a research organization that serves the U.S. Military.

So read on, understanding that all our "what-if?-ing" serves neither as prediction nor perception management by the U.S. Naval War College. Like everyone else on this planet studying Y2K, we're groping for answers. Yes, we've done our effort in a rather comprehensive fashion, and yes, we are experts at thinking about future events. But please don't approach this analysis as "cookbook," but rather as "primer." The confidence we seek to instill in readers—key decision-makers and average citizens alike—is one of comprehending the potential scope and complexity of the scenario, and *not* of reducing the Millennial Date Change Event into a crude or simplistic "one-to-ten scale" type of crisis management strategy.



There's nothing wrong with being deeply concerned about Y2K on a global scale after you've read our report, but if you're fearful or panicked, then you haven't really understood what we said.

---

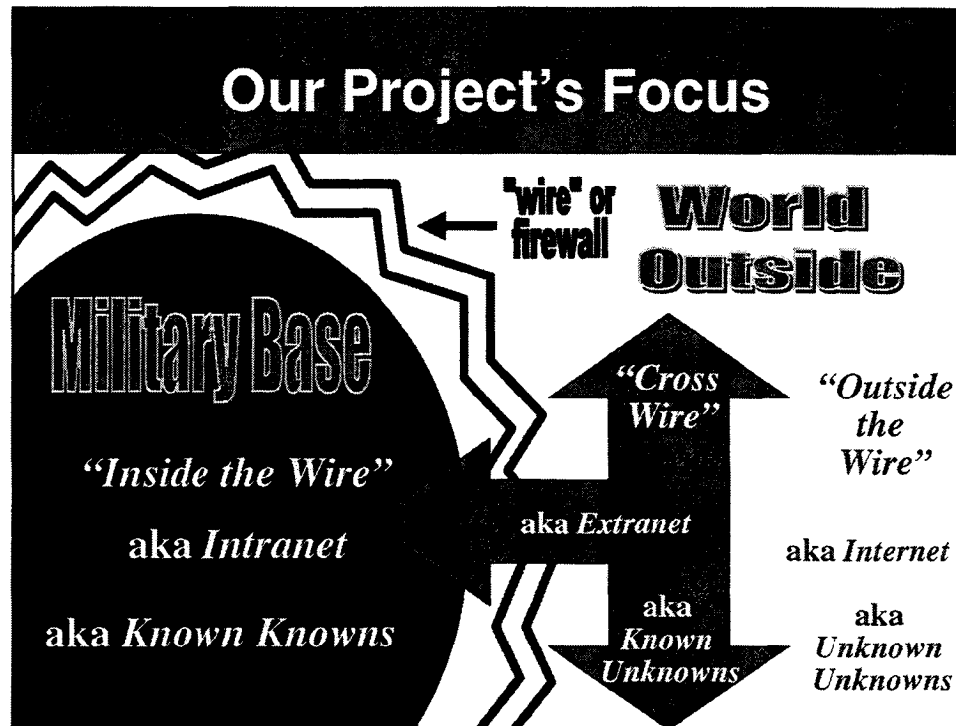
## II. Our Big Picture Approach

### DoD Preparations for Y2K and Where We Fit In

We won't be offering any "official history" here, nor any insider critiques of U.S. Government efforts to prepare for Y2K. We just want to be up front and clear in explaining how we see our work fitting in with the rest of DoD's broad, long-term effort that stretches back several years. By and large, we're latecomers to this party, having only begun our research effort in August of 1998. To the extent that we've moved closer to the head of the pack on scenario planning, it's because we've focused on the broad dynamics of how the Millennial Date Change Event may possible unfold—*not on the technical aspects of network, software, or embedded chip failures directly caused by Y2K, nor on any remediation efforts to prevent such failures*. In short, we're pure crisis management in focus, which is why our analysis has attracted particular attention within the intelligence community.

DoD preparations for Y2K through the spring of 1999 have almost exclusively focused on dealing with what we'd describe as the *known knowns* (see Slide 1), or identified problems that have identified answers. For DoD, it's useful to think of these problems—albeit in a highly reductionist manner—as those that occur *inside the wire* ("wire" referring to that which separates the military world from the civilian world, or the fences that typically surround military bases), meaning those activities that occur within bases or between operating platforms (e.g., ships, planes, transport vehicles). This is the classic remediation focus one would expect: making sure *all our systems work individually and collectively*. By most reasonable measures, DoD has this problem set well in hand—and it only makes sense that it would. It's a huge organization with lots of money and lots of responsibility.

Starting early this year, DoD attention has turned increasingly to the subject of host nation and U.S. local community support to military bases—namely, utilities such as electricity, phone systems, and sewer. We like to describe this set of potential issues as the *known unknowns*, meaning identified problems without easily identified answers. If the *known knowns* can be thought of as existing *inside the wire*, then the *known unknowns* are basically those Y2K issue areas that *cross the wire* that separates the military and civilian worlds. From DoD's perspective, no matter how well they remediate their own systems and networks, there's still the huge question of how much their base operations rely on host nation support. This will be a subject of intense DoD effort and planning as the rest of the year unfolds.



Slide 1: *Inside the Wire vs. Cross Wire vs. Outside the Wire Perspectives*

Our project's work really has nothing to do with either of those first two problem sets, for what we're really concerned with is what can still go wrong *beyond the wire*. Moreover, we're not concerned with bases located within the U.S., as Y2K crisis management within the U.S. will be led by the Federal Emergency Management Agency in conjunction with a host of state and local government agencies. Thus, our study's focus is exclusively on what could go wrong during Y2K *beyond the wire in foreign countries*, or crises to which DoD could be called upon by National Command Authority (i.e., the White House) to respond. This is the real set of *unknown unknowns*, for while most Y2K analysts will agree that we have a fairly decent read on what will or will not likely happen in the U.S., our sense of what could or could not go wrong abroad is far weaker.

Historically, the U.S. responds to about 5 to 8 major crises a year around the world with some sort of significant military effort (e.g., ships dispatched, troops deployed, planes fly sorties). Typically, 2 to 3 of these crises are ongoing situations where we continue operations begun in a previous year, like those today in the Former Republic of Yugoslavia or Iraq. The rest tend to be "peaks in messes," meaning ongoing bad situations that flare up or deteriorate to the point that the U.S. decides to intervene militarily in some manner, such as recent forays into Haiti or Somalia.

Of course, the \$64,000 question with Y2K and the Millennial Date Change Event is, "Is this confluence of elements likely to create a higher-than-normal crisis load for DoD over the year 2000?" For example, instead of looking out on the world and seeing the usual 10 to 20 crises and picking 5 to 8 for response, does the U.S. Government look out over the course of 2000 and see some larger number of crises, and, if so, do we pick the same "top 5 to 8?" Or a different "top 5 to 8?" (meaning our calculus of national interest might be changed during this unusual period). Or do we try to do more than the usual effort? In short, how important may Y2K turn out to be in terms of U.S. foreign policy—both in the short term and over the longer term?

No one can offer precise answers to these questions. What we can say, though, is that our analysis to date hasn't uncovered any serious evidence that what DoD could be called upon to do in terms of crisis response would be dramatically different from what we've done in the past—namely, disaster relief and humanitarian assistance. Of course, there's always the chance that crisis will generate conflict, but again, we don't foresee any new species of crisis here, but rather the types of situations with which DoD has great experience.

We believe our analysis offers particular utility in alerting military planners, decision makers, and operational commanders to the sorts of broad scenario dynamics they may encounter if they are called upon to engage in military operations in response to Y2K-related crises, or even non-Y2K-related crises that occur during the same time period. So while the missions may not change, the local and regional environment within which those missions occur may experience social, political, economic and infrastructural dynamics that are unusual and linked to either Y2K or the larger Millennial Date Change Event. Moreover, to whatever extent our analysis of generic Y2K and Millennial Date Change Event scenario dynamics illuminates potentially similar dynamics within the U.S., additional understanding may accrue concerning the overall stress level that may occur "back at the home front."

Again, none of our material here is meant to be predictive in the sense of providing a step-by-step "cookbook" approach to Y2K and Millennial Date Change crisis management. Our fundamental goal in collecting and synthesizing this analysis is to avoid any situation where U.S. military decision makers and/or operational commanders would find themselves in seemingly uncharted territory and declare, "I had no idea . . ." We can't and won't tell any regional CINC staff how to run a military operation during Y2K's unfolding or the Millennial Date Change Event. They know far better than we do how to proceed in such real world contingencies. All we can do is alert them to the particular scenario dynamics that may come together during this potentially unusual global experience.

## A Process View of Y2K

"Y2K—The Event" will feature a distinct build-up phase (already begun), a peak period we consider "THE crisis," and an "end" phase in which the crisis unwinds either by its own accord or, more likely, by decree. Either governments will declare that the "crisis has passed" *or* some other crisis will arise and capture our attention. Slide 2 presents another way of thinking through the process of Y2K's build-up, unfolding, and end.

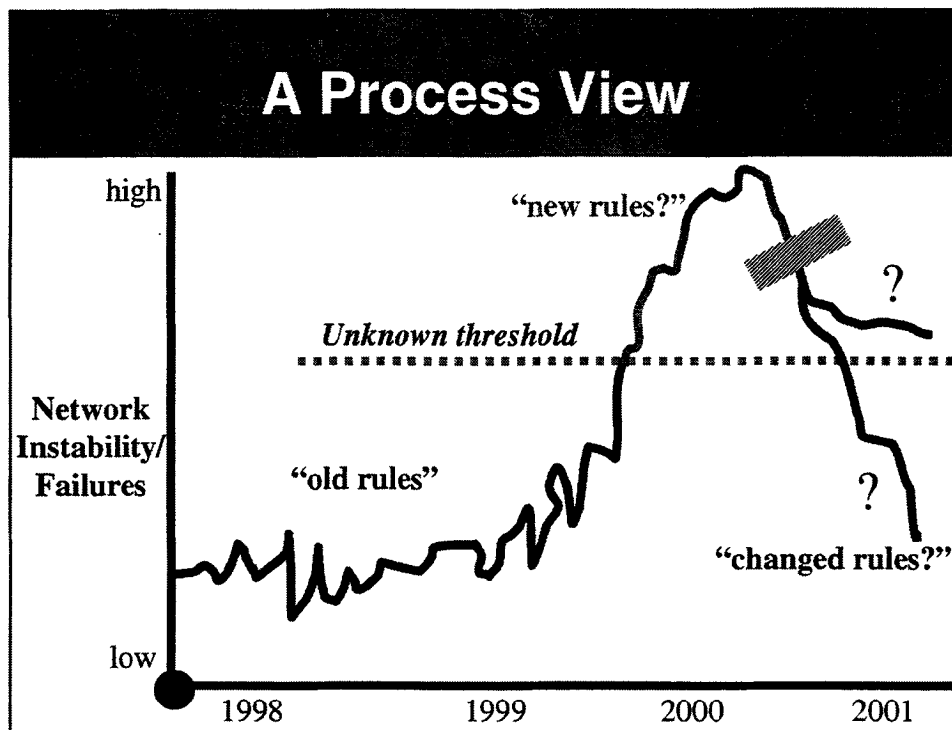
The vertical axis of Slide 2 speaks to Network Instability/Failures, meaning the sorts of computer and network failures we've all experienced in our daily lives. The horizontal axis offers a timeline from 1998 to 2001.

As we move from left to right, the relatively low level of network instability and/or failures that we show for 1998 represents life as we know it—i.e., computers and networks break down with a certain frequency that we have come to know and accept. A big part of that acceptance is the "rule set" we have developed for dealing with these failures, such as "Always check by phone if the pager seems down," or "Always follow up with a phone call when the e-mail doesn't seem to go through." We'll call these familiar rules of thumb the "old rules," which we've developed as workarounds for familiar failures. These are our effective coping mechanisms, to use a psychological term.

The key uncertainty for 1999 is the extent to which the level of network instability/failures begins to rise over the course of the year as we get closer to dateline 010100 (six-digit code representing the first day of January, 2000, as in, *ddmmyy*). If Y2K turns out to be a significant experience, then at some point in late 1999 or perhaps the first few days of 2000 the frequency and/or severity of the network instability and/or failures will reach some unknown threshold past which the "old rules" will no longer seem to apply. At that point, society would—in effect—develop a "new rule set," or "new rules" that apply to the dramatically altered parameters of the perceived crisis situation—however defined.

Our project is largely concerned with uncovering and understanding the potential "new rule set" that would ensue *if* Y2K, when combined with the Millennial Date Change Event, turns out to cause a significant and unprecedented rise in network instability for an *extended* period of time. Now, we can debate what the word "extended" means, but for our analytical purposes, it would be a length of time that exceeds what a reasonable citizen might expect in terms of network, economic, social, and government service disruptions arising from the "3-day snowstorm" measure that many advocate as a planning parameter for Y2K. Any unfolding of Y2K that doesn't create a lengthier array of significant disruptions for any area, country, or region, is unlikely to generate a "new rule set."

Finally, once the Y2K Event plays itself out (signified in the slide by the break in the chart line) and the failure/instability rate begins to decline, the question in terms of Y2K's



Slide 2: A Process View of Y2K

long-term legacy is whether or not we return to the "old rules" associated with the previously understood standard of network instability, or whether we settle in on some "changed rule set" engendered by our experiencing of the Y2K Event. In large part, that will depend on the extent to which we come to understand Y2K as either a one-time event unique in human history or a preview of what "network instability" (and its associated crises) may evolve into as we move ever deeper into a period of history where individuals, communities, countries, and regions of the world become more interconnected and interdependent. In short, if globalization and networking represent the future, maybe Y2K has far more to teach us about that future than we might think if we view it as nothing more than the "last stupid act of the 20th Century."

## Millennial Mania as a Key Element of the Millennial Date Change Event

In this section, we'll define Millennial Mania as corresponding to one of our previously noted elements of the Millennial Date Change Event—namely, the *Millennial Event in its extremist form, i.e., characterized by expectations of profound and cataclysmic global*



*change, typically associated with apocalyptic visions involving interventions by a deity or supernatural force.* Having to define this element, we might seem to be relegating it to the extreme edges of society, and, to a certain extent, we are.

However, given the simultaneity of Y2K's unfolding and the opportunity afforded by the Millennial Date Change Event for a portion of the public to interpret Y2K's meaning and causality through the prism of an apocalyptic perspective, the Millennial Mania element may—in effect—"pour fuel on the fire," heightening inappropriate or counter-productive responses to those direct Y2K failures that may occur. This can happen in a variety of ways, with the three most important avenues being:

- Tendency to extrapolate direct Y2K failures into "overwhelming evidence" of the collapse of society
- Propensity to attribute causality of "fellow traveler" failures to Y2K, thus feeding the "overwhelming evidence" of the collapse of society
- Capacity to behave in response to such "overwhelming evidence" in ways that, in turn, lead to cascading network failures or related societal breakdowns where none would have otherwise occurred, which subsequently provide even more "overwhelming evidence" in a self-fulfilling fashion.

It is the last concept that we would like to highlight—namely, the notion of "iatrogenesis," which is narrowly defined as *the unintended side effects resulting from treatment by a physician*, but which we use more broadly to mean *average people doing stupid things during stressful times* (although the notion of unintended side effects caused by a true expert is useful as well—namely, the mistakes created by software remediation).

As is readily apparent to anyone who's tracked the Y2K debate, there are many Y2K "physicians" currently on the scene, many of whom have little understanding of information technology, but who are nonetheless offering all sorts of "advice"—usually for a fee. By and large, we are not talking about IT firms and consultants in the business of remediation or commercial crisis management, but the relatively narrow group of self-proclaimed experts who offer frightening predictions regarding Y2K effects, as well as ways to "weather the storm"—usually by purchasing their products or services.

In addition to the hucksters and outright scam artists, there is a relatively small but highly vocal and well connected (over the Internet) group of individuals and organizations promoting all sorts of apocalyptic interpretations of Y2K's meaning and causality. Some seek remuneration, but many do not, as they firmly believe—in their millenarian fashion—that the "signs" of the "end times" are somehow foretold in Y2K's onset and unfolding. The vast majority of these "physicians" tend to predict great harm will come to those elements of society for whom they have historically shown great contempt. In other words, these "experts" tend to warn of disaster for *those unlike themselves*, with "unlike" being defined in terms of religious beliefs, racial or ethnic categories, political attitudes, social mores, sexual orientation, and the like. The tendency of some of these "experts" to

attribute Y2K's alleged destructiveness to the "evilness of *their* ways" is unmistakable and deplorable.

Such fear mongering "physicians" prey on those intimidated by information technology in general, and in particular those looking for external guides to help them interpret and understand Y2K's meaning and causality. The impact this small but influential group of "experts" may have on societal response to Y2K's onset and unfolding is extremely difficult to predict. Mass media and elites in general tend to grossly overestimate the panic factor in natural and man-made disasters, as proven time and time again throughout history. Moreover, the tendency of elites to censor the flow of information out of fear of panic is often a far larger source of instability than the crisis itself. In that sense, it is less the power over mass behavior that fear-mongering "physicians" or "experts" actually exert during Y2K's onset and unfolding, than the power they *seem* to exhibit in the preceding months and weeks that may negatively impact elite decision making regarding the transparency of government preparations and plans for dealing with whatever crisis may actually ensue. In short, the most profound iatrogenic effect these "physicians" or "experts" may have could be on elite behavior vice mass behavior—again, in that self-fulfilling manner that exemplifies iatrogenesis.

For further insights into Millennial Mania and the forms it may take surrounding Y2K and the Millennial Date Change Event, we recommend the following:

- Visit Boston University's Center for Millennial Studies' web site ([www.mille.org](http://www.mille.org)) for more information regarding millenarian or apocalyptic groups and their potential for disruptive or iatrogenic behavior in the coming months; the site provides many good links in addition to numerous interesting and illuminating interpretations of ongoing social response to both Y2K and the Millennial Date Change Event
- Rent any of the following movie videos for glimpses into a variety of extreme responses or emotional dynamics that segments of society may exhibit during Y2K and/or the Millennial Date Change Event:
  - *The Rapture* (1991), on why certain people are attracted to visions of religious-based apocalypse
  - *The Trigger Effect* (1996), on how stressful situations can lead to iatrogenic behavior due to "battle fatigue"
  - *The X-Files* (1998), on "paranoia" (you can figure out your own definition of that word) over government conspiracies, cover-ups and the abuse of political power during crises
  - *Deep Impact* (1998), on divided loyalties in the face of looming crisis and popular responses to the notion of "The End of the World As We Know It" (AKA, "TEOTWAWKI," a broad theme that runs through much of the apocalyptic interpretations of Y2K's potential global impact).

And if none of that jars your imagination regarding Millennial Mania, then just consider that astronomers are predicting one of the most violent periods of solar flare activity in recorded history for the period January through March 2000. So, if you're looking for a sign from above . . . you'll get it.

## **The Biggest Picture View of Y2K's Potential Impact on Global History**

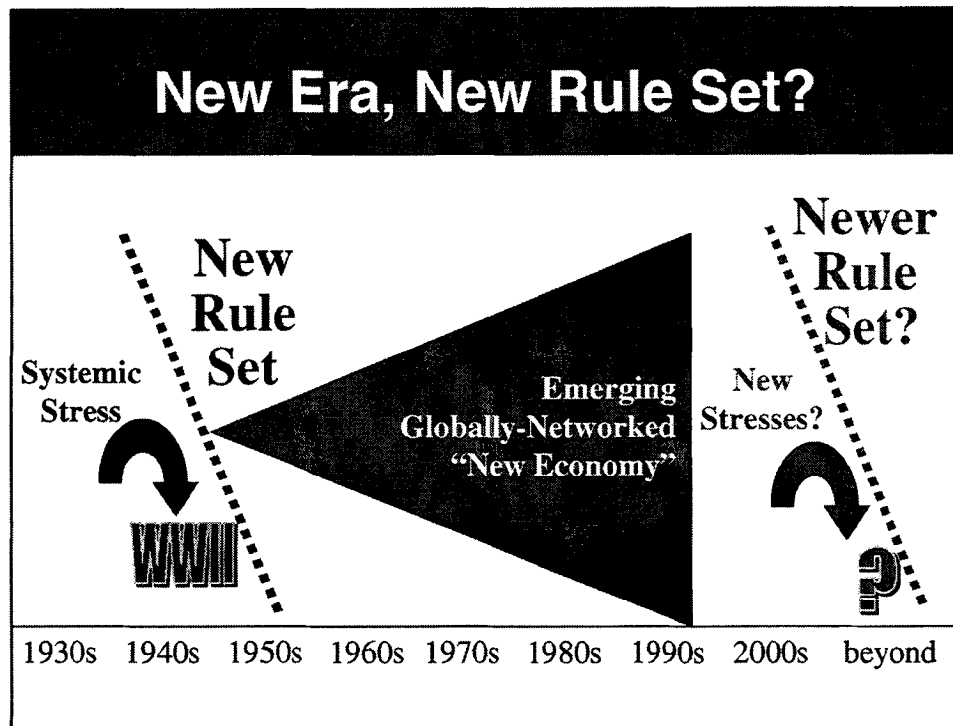
The Y2K Event comes at what may be a pivotal point in global history. We'll explain this bold statement using Slide 3.

The global rule set that has marked international relations throughout the Cold War period and into the 1990s finds its roots in the systemic stresses of the 1930s—namely, the Great Depression and the rise of fascism in Europe. These twin developments quickly segued into the Second World War, from which came the notion that "never again" would the international community engage in the sort of self-destructive behavior (e.g., economic protectionism) that both led to and exacerbated the Great Depression, and by doing so laid much of the groundwork for World War II. Based on that "never again" spirit, the global system's great powers, led most notably by the United States, attempted to "firewall off" the experiences of the 1930s and early 1940s by creating a new global rule set, whose main attributes were exemplified by such international organizations as the General Agreement on Trade and Tariffs, the United Nations, the International Monetary Fund and the World Bank.

This new global rule set gave birth to the second great period of economic globalization (the first being roughly from 1870 to 1929), creating what we've eventually come to know and identify as the globally networked "New Economy." This New Economy features, as Thomas Friedman has noted in his book, *The Lexus and the Olive Tree* (New York: Farrar Straus Giroux, 1999, pp. 39-58), three critical democratizing processes:

- Democratization of global finance
- Democratization of global communications
- Democratization of global technology.

As this New Economy emerges on a global scale, it has begun to feel some "growing pains," most notably in the Global Financial Crisis of 1997-98 (beginning in Asia and spreading to Russia and Brazil), leading some to question whether the Global Rule Set of the early postwar years is still appropriate for the world in which we currently live. Granted, the now seemingly "old" Global Rule Set of the late 1940s and early 1950s succeeded beyond the wildest dreams of its progenitors. It not only outlasted the main threat to global stability of its time, the Soviet Bloc, but also created the greatest period of global economic advance in history, not to mention the longest period of great power



Slide 3: The Biggest Picture View of Y2K

peace in the 20th Century. However, as states and their economies become increasingly intertwined in this information technology-driven New Economy, legitimate questions arise as to whether or not a new Global Rule Set is in order.

Naturally, the United States is not particularly enamored with the call for a new Global Rule Set, for it is doing quite nicely in the current set and most of the calls for new rules typically center on placing restrictions on the free flow of international capital, something the U.S. does not wish to see for reasons of its obvious economic success over the course of the 1990s. If, however, Y2K were to induce serious global economic disruptions, coming as it does on the heels of the Global Financial Crisis of 1997-98, then it is possible that international sentiment for some aspects of a new Global Rule Set, however defined, would grow so powerful that even the United States might find it advantageous to shape its emergence rather than delay or prevent its emergence.

Could Y2K play the role of the "straw that breaks the camel's back?" At this point, it seems like a long shot, and yet, 1989 looked to be a rather ordinary year until 1990 rolled around and we realized the Cold War was essentially over. In short, we rarely have the opportunity to schedule moments of global historical importance—they simply appear on their own and usually elicit our great surprise. The fact that Y2K is indeed a scheduled moment in history only adds to its mystery, but in the end, if Y2K proves to be an histori-

cal turning point between one era and the next, it won't be because of what Y2K is, but because of what it told us about the status quo and the need for change. In short, it's not what Y2K destroys that will be important, but what it illuminates.

---

# III. A Series of Y2K Onset Models

## Explaining Our X-Y Axis

Our X-Y Axis (shown in Slide 4) begins with two simple questions:

- Horizontal axis asks the "What?" question: What is the nature of the Y2K Event?
- Vertical axis asks the "So What?" question: What is the impact of the Y2K Event?

There is a huge difference between these two questions, for the first question focuses on cause, while the latter focuses on effect.

One way we like to differentiate between the two questions is to employ a medical analogy. Think of the horizontal axis (What? question) as the nature of the trauma or illness and the vertical axis ("So What? question) as the patient's overall health. Two extreme examples show why this analogy is illuminating:

- Example 1 is an elderly man who is stricken with a very slow growing bladder cancer. While this elderly man could have lived with this cancer for several years, the stress of his hospitalization, exploratory surgery, and the frightening diagnosis stresses his already fragile system to the point where he suffers a stroke and is dead within two weeks as a result of major organ failures cascading throughout his system. To sum up, while the initiating event (bladder cancer) was more minor than major (placing it on the left side of the horizontal axis below), the man's overall system robustness was weak (placing him on the lower side of the vertical axis). The medical outcome was—irrespective of its modest origins—disastrous.
- Example 2 is a two-year-old child struck with a very aggressive kidney cancer that—by the time of diagnosis—has spread to both her lungs. Other than that, though, the child is in excellent health, and as such, is more than able to survive the surgeries, radiation, and months of chemotherapy with no lasting negative effects of clinical value. To sum up the child's case, while the initiating event (kidney cancer) was more major than minor (placing it on the right side of the horizontal axis), the child's overall system robustness was strong (placing her on the higher side of the vertical axis). The medical outcome was—again, irrespective of its profound origins—quite positive.



These two very different medical case histories, drawn from the author's family history, highlight the importance of juxtaposing the "What?" and "So What?" questions to create the four quadrants of the X-Y axis, for it is not enough simply to ask how bad Y2K may be. Given how bad it may be (i.e., how many computerized systems fail), Y2K's ultimate impact will depend greatly on the targeted system(s) in question.

Looking at Slide 4, we then explain our X-Y Axis as follows:

- The horizontal axis, asking the "What?" question of the Y2K Event, posits the minor extreme on the left as being "Y2K events are discrete and episodic" and the major extreme on the right as being "Y2K event is widespread and sustained."
- The vertical axis, asking the "So What?" question of Y2K's impact, posits the minor extreme on top as being "Systems are robust," and the major extreme on the bottom as being "Systems are vulnerable."

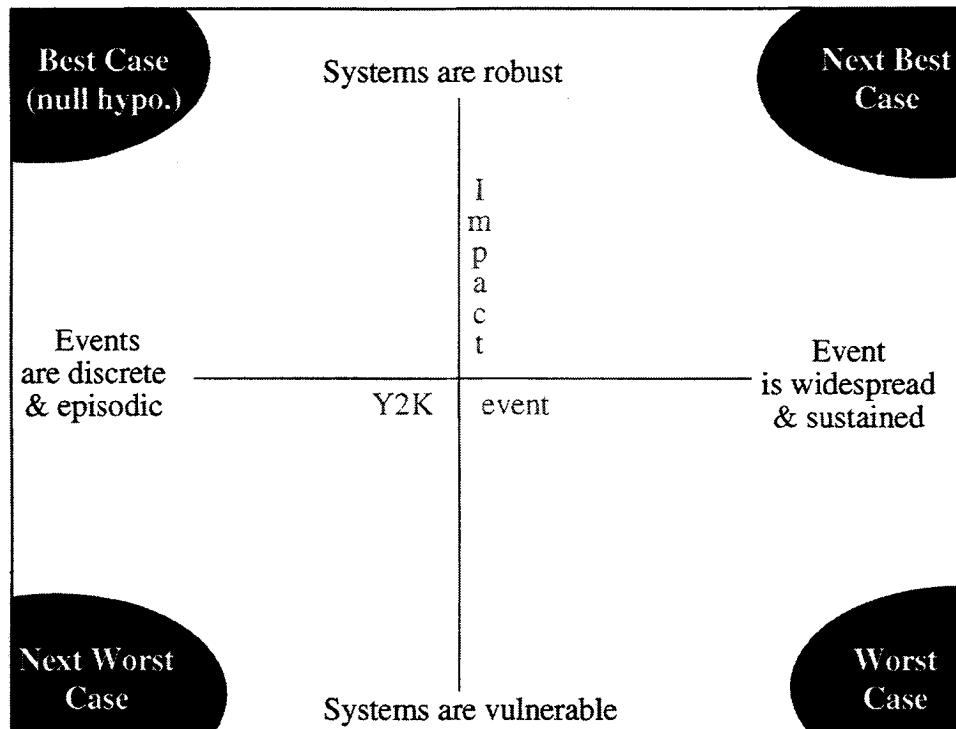
Two caveats are in order:

- By "Y2K Event(s)," we refer only to network failures directly attributed to Y2K or those caused via subsequent cascading system failures, to exclude any social, economic, or political responses that exacerbate or reduce failure rates.
- By "Systems," we refer not only to a country's network systems (broadly defined to mean any network that moves something—e.g., bytes, people, electricity), but also its political, economic and social systems, with the key attributes of robustness being:
  - Distributiveness
  - Recovery capacity
  - "Workarounds" capacity
  - Trust "capital."

Having defined the extremes of our axes, we break down the four quadrants in the following manner:

- Best Case is when Y2K events are discrete and episodic and systems are robust
- Next Best Case is when the Y2K event is widespread and sustained, but systems are robust
- Next Worst Case is when Y2K events are discrete and episodic, but systems are vulnerable

- Worst Case is when the Y2K event is widespread and sustained and systems are vulnerable.

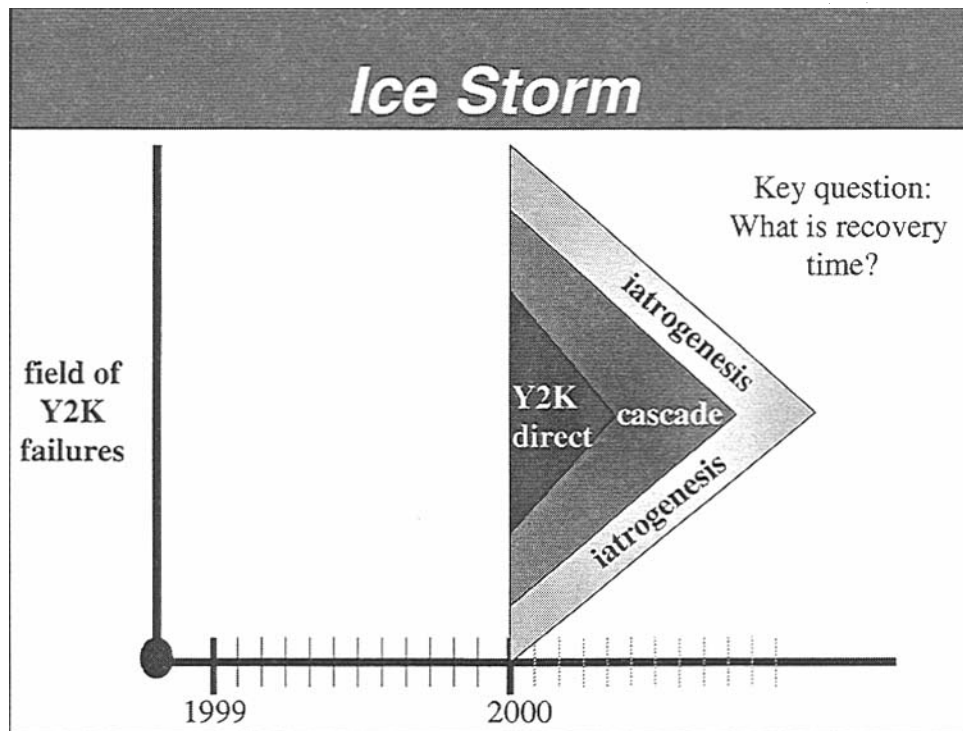


Slide 4: The X-Y Axis for Y2K Onset Models

## Y2K Onset Model #1: The *Ice Storm*

The *Ice Storm* onset model is depicted in Slide 5.

In the embedded chart, the vertical axis defines a "field of Y2K failures," meaning we're not going to offer any percentages or "hard numbers" here, just a rough notion of overall failure saturation. Along the vertical axis we display the years 1999 through 2001, with the months of 1999 noted in solid-line marks and the months of 2000 noted in dashed-line marks. The difference between the two markings is meant to suggest that while we may feel we have a firm grasp of appropriate time units for the timeline leading up to 010100, perceptions of time's passing once we pass through the 010100 threshold may vary greatly depending on locale. For example, the subjective time unit of note for Wall Street at the beginning of January may be the first day of trading—a mere several hours' time, whereas the subjective time unit of note for a sheep herder in a less developed



Slide 5: The *Ice Storm* Onset Model

country may be as long as until the first time he brings his sheep to market—possibly several weeks.

The *Ice Storm* onset model offers the classic TEOTWAWKI view of Y2K: it hits *en masse* on or about 010100 and strikes virtually every aspect of society. To the extent that such a model may seem to hold true on a perceptual basis in any one locality or region (meaning, for all practical purposes, it seems as though all systems are impacted to some disabling degree), we posit that the *Ice Storm*'s components are logically broken down into three categories:

- Direct Y2K failures
- Cascading system failures resulting from the direct failures
- Iatrogenic crisis management or social responses that exacerbate the cascading failures or trigger new threads.

While this model held implicit sway over much of the Y2K debate in 1998, it has receded in prominence over the course of 1999, as remediation efforts make clear that this is not a useful universal model. Having said that, however, we believe the model retains great validity for understanding pockets of significantly damaging Y2K impact that may occur

around the world, meaning those areas where—for all practical purposes—the TEOTWAWKI notion may well emerge among significant portions of a population battered by widespread network failures.

Of course, even here we're still talking only about the perceived onset, and not some sustained environmental status that would realistically drag on for months. As such, the key question for the *Ice Storm* onset model is, "How fast can the society or economy in question recover by necking down the failure rate to some level commensurate with reasonably sub-optimal functioning (meaning, for many around the world, the return to "life as we know it")?"

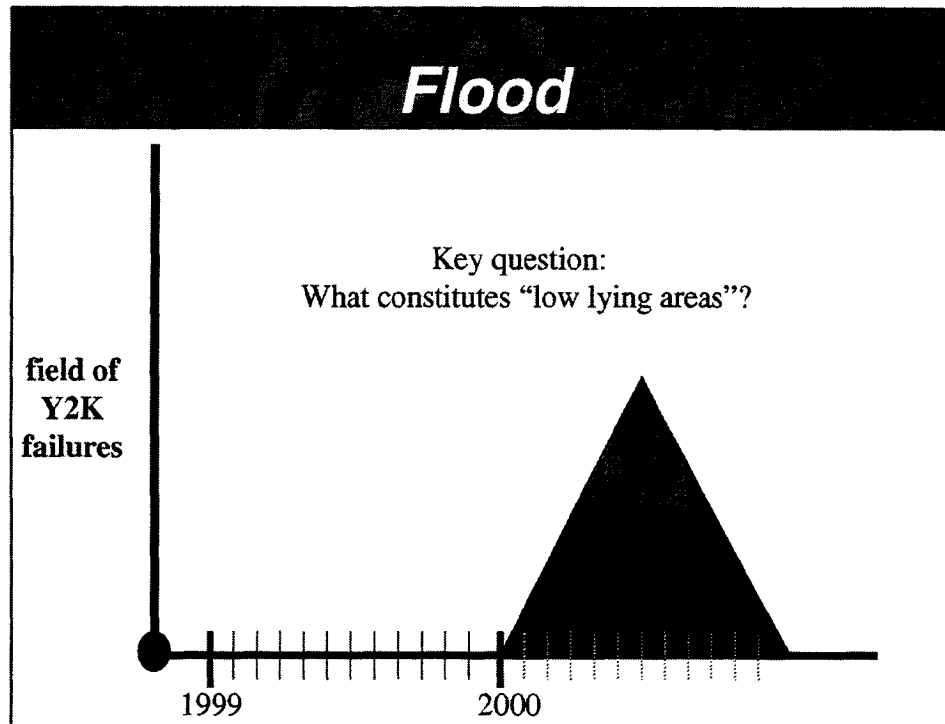
## Y2K Onset Model #2: The *Flood*

The *Flood* onset model is depicted in Slide 6.

The *Flood* onset model depicts a slow but inexorable bulge of network failures that first rises above the usual "background noise" level on or about 010100 and then expands for something in the range of the first six months of 2000, peaking near the end of the 2nd Quarter or at some point in the 3rd Quarter. In some ways, we could suppose the same breakdown of elements (direct, cascading, iatrogenic) here as with the *Ice Storm* model, but because of the greatly extended timeline (thus allowing for more effective crisis management and network triage), we limit our description here to direct and cascading network failures, thus positing a peak failure rate somewhere in the range of 50 percent of all networks.

As such, the *Flood* model gets nowhere near the TEOTWAWKI pain range, but instead describes something more akin to a significant economic downturn, most likely corresponding to popular perceptions of a recession or financial market "correction." In that manner, the *Flood* model possibly describes a more profound economic impact than the *Ice Storm*, which, while it is a shock to the system, is probably of shorter duration. So, like the *Ice Storm*, the *Flood* model involves an interrelated sequence of network failures, albeit with a far smaller immediate impact on the overall functioning of society.

In keeping with the weather analogy, the key question for the *Flood* model is, "What constitutes a 'low-lying area'?" One example of a potential low-lying area would be manufacturing, whose network failures would not likely be centered on the 010100 threshold, but rather build up over time as production continued throughout 2000. Another could be medical supplies, especially the production and distribution of key pharmaceuticals. Still another might be the processing and distribution of clean drinking water.



Slide 6: The *Flood* Onset Model

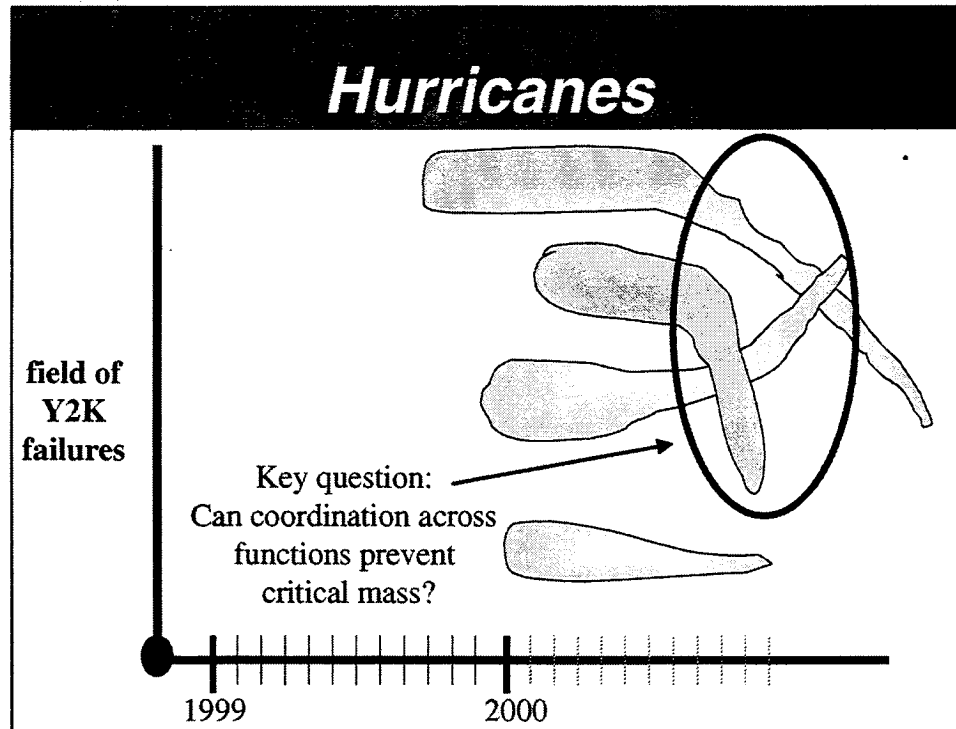
### Y2K Onset Model #3: The *Hurricanes*

The *Hurricanes* onset model is depicted in Slide 7.

The *Hurricanes* onset model presents a series of sectorally limited (meaning unconnected across sectors) but relatively lengthy (meaning some cascading effect) constellations of network failures. In effect, this model is a hybrid of the *Ice Storm* and *Flood* models. The *Hurricanes* model packs the same immediate punch as the *Ice Storm* model, albeit in isolated "low-lying areas" (echoing the *Flood* model), thus limiting the overall impact on the functioning of a society.

The *Hurricanes* model speaks more to the "winners and losers" approach to thinking about Y2K's ultimate impact: some sectors of society will seemingly get off scot-free, while others will seemingly suffer great damage. The key difference with the *Flood* model is the lack of interrelation and simultaneity, so rather than employing the economic language of "downturns," we're more likely to describe "shake-ups" in one or another industry.

The same approach to identifying vulnerable sectors that one uses with the *Flood* model would apply here, although in an overall sense, the *Hurricanes* model is probably best



Slide 7: The *Hurricanes* Onset Model

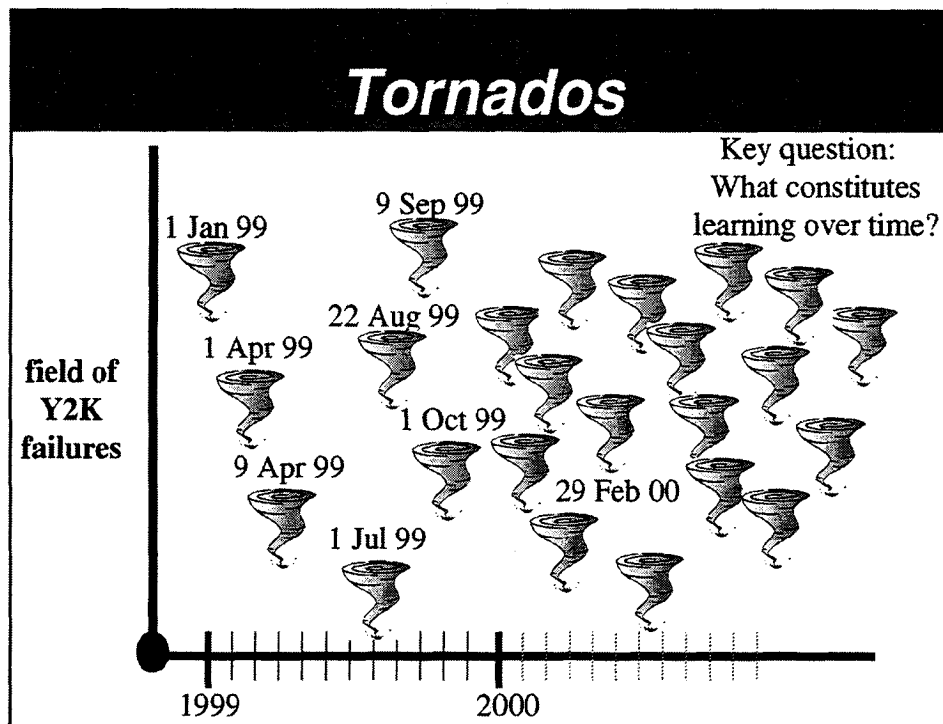
used to think about countries whose remediation efforts have been weak, for here we run into the notion of over-confidence possibly leading to poor crisis management preparation. If such "poor remediators" turn out to be far more vulnerable than they realize, then the key question becomes, "How can coordinated triage and crisis management avert the appearance of a critical mass of substantial—yet still relatively isolated—network failure clusters?"

## Y2K Onset Model #4: The *Tornados*

The *Tornados* onset model is depicted in Slide 8.

The *Tornados* onset model refers to a "season" of sectorally and temporally limited Y2K-induced network failures. This model is the closest to a null hypothesis of Y2K's overall impact, for, in many ways, it describes life as we know it, albeit with a higher-than-average failure rate. The *Tornados* model can likewise be thought of as the "key dates" model, for the two go naturally hand-in-hand when one seeks real-world evidence of significant network failures that either produce serious disruptions of service or require extraordinary efforts at repair. For if such key dates come and go without displaying any





Slide 8: The *Tornados* Onset Model

significant failures, meaning they're so big they can't be hidden by the service providers in question, then these Y2K milestones pass by without registering significant values on any sort of TEOTWAWKI scale, becoming the Y2K equivalent of a tree falling in the forest when no one's there to hear it.

The key dates approach does correspond nicely with the Gartner Group's predictions of Y2K failure rates rising and falling over the course of 1999 and through the year 2001, but the big deficiency of this model to date has been the lack of any stunning failures on key dates that have already passed. For example, no failures featuring major negative impact occurred on 1 or 3 January, the first day and business day, respectively, of 1999. The start of many fiscal year programs on 1 April also failed to reveal any serious disruptions for the governments involved. The so-called "nines" problem that was slated to appear on 9 April likewise produced no failures of great societal value in any country around the planet. Most recently, the 1 July threshold came and went with no apparent damage to the 46 U.S. states whose fiscal years began that day.

Meanwhile, Cap Gemini America, the computer consulting firm, declares on the basis of their recent survey of Fortune 500 companies and a smattering of U.S. government agencies that close to three-quarters of the respondents report experiencing a Y2K-related failure through the first quarter of 1999. But if these firms are having these failures and

none are making any headlines, how is that much different from everyday life as we know it? Aren't private firms and government agencies experiencing network problems on a fairly regular basis, and just as regularly keeping such failures under wraps? The key missing data involve how much different 1999 is turning out to be compared to any previous year, meaning what is the "instability added" from Y2K? And that's the data we haven't found anywhere yet.

Having said that, the key question for the *Tornados* model remains, "What constitutes good learning over time?" For example, should our confidence grow due to the lack of Y2K headlines stemming from the key dates already passed? Or should we ignore most if not all of that success, especially for a pure fellow traveler such as the "nines" problem? After all, we can get fixated on Y2K key dates all through 1999, get through them all quite nicely, and still suffer significant tumult on 010100. Uneventful key dates make that seem less likely, but don't rule out it out by any means.

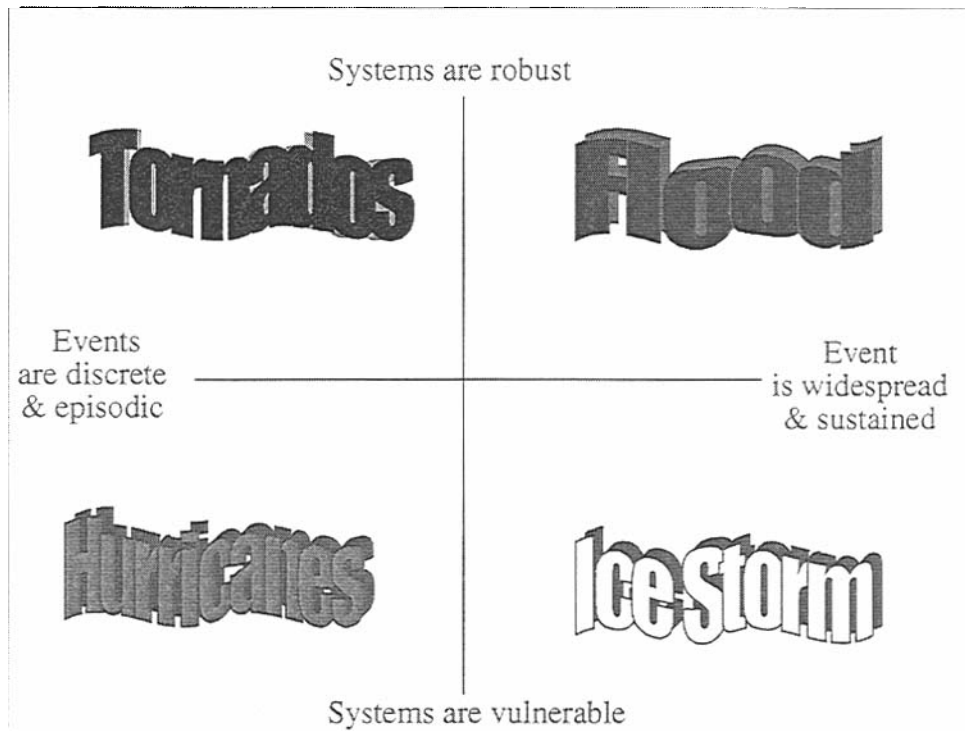
## Onset Models Leading to Generic Y2K Outcome Scenarios

Of course, none of the four onset models are likely to hold sway for any one region's entire Y2K experience, and in that sense, we are likely to see versions of all four models occurring simultaneously around the planet at various points in the Y2K Event. As ideal types, the four models are designed to help the reader disaggregate the complexity presented by Y2K's myriad of possibilities, rather than provide a "pick one of four" analytical choice that would invariably prove false and pointless.

Slide 9 arrays the four onset models on our X-Y axis, and the placement should seem fairly intuitive given our descriptions:

- *Tornados* represent the "Y2K events as discrete and episodic" and "systems are robust" quadrant, meaning a season of relatively isolated and concentrated damage that follows little rhyme nor reason to the extent that we can trace causality.
- *Flood* represents the "Y2K event as widespread and sustained" but "systems are robust" quadrant, meaning a rising tide or deluge of damage that follows the logic of systematic vulnerability, i.e., the low-lying areas analogy.
- *Hurricanes* represent the "Y2K events as discrete and episodic" but "systems are vulnerable" quadrant, meaning a season of somewhat isolated but wide-swath damage that follows the logic of either poor remediation or unforeseen vulnerabilities—basically one in the same.
- *Ice Storm* represents the "Y2K event as widespread and sustained" and "systems are vulnerable" quadrant, meaning a seemingly pervasive or all encom-

passing damage pattern that is inescapable, but one that at least reveals itself in its entirety with great speed, thus facilitating recovery.



Slide 9: The Onset Model Arrayed on the X-Y Axis

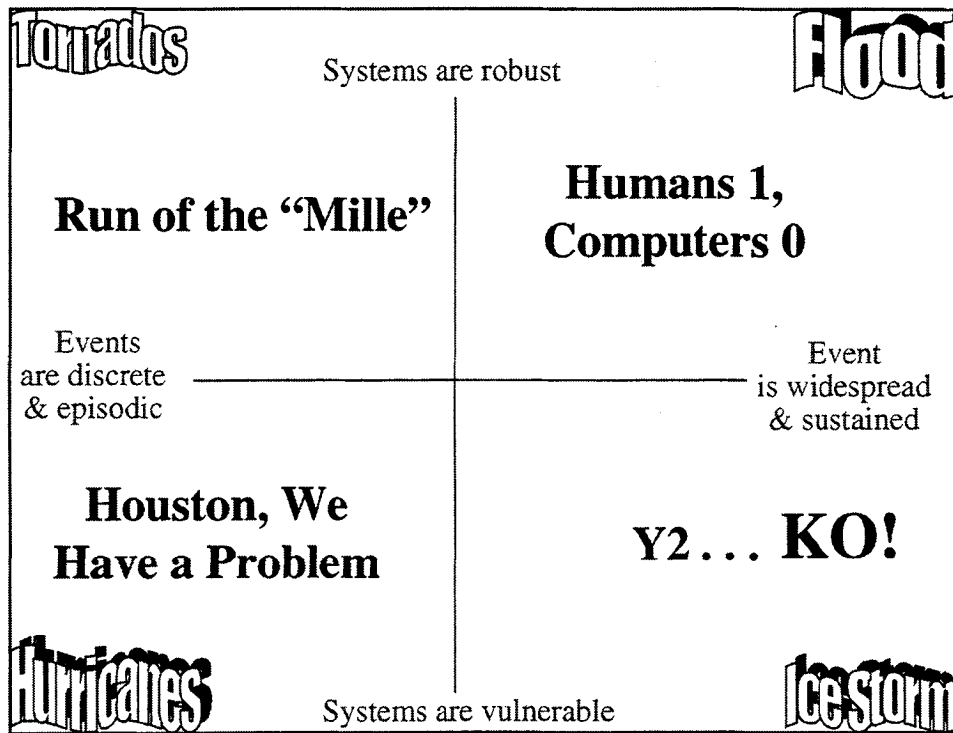
Again, our rationale in presenting such onset models is not to encourage a "pick one" mentality, but rather to break down the abstract nature of the potentially universal problem set into a series of weather analogies that are far more easily understood by the average citizen—not to mention your average elite decision maker.

Slide 10 presents a series of outcome-focused Y2K scenario titles arrayed along our X-Y axis. By pairing them up with our onset models, we—in effect—offer a "coming and going" view of the Y2K Event (leaving the "guts" of our Y2K analysis for the section on Scenario Dynamics).

- *Run of the "Mille"* refers to the Best Case Scenario, meaning Y2K comes in bits and pieces and we prove far more robust than we give ourselves credit for. So it's "run of the mill" in that we take Y2K in stride, but *Run of the "Mille"* in the sense that the Millennial Date Change Event still exists at the core of the Y2K null hy-

pothesis. Thus, in this scenario, whatever social instability occurs around the 010100 threshold is more driven by millennial elements (e.g., apocalyptic-driven behavior, world's largest party, great religious feast) than by actual Y2K-driven network failures. Humanity emerges on the far side of this "crisis" wondering what all the hype was about.

- *"Humans 1, Computers 0"* refers to the Next Best Case Scenario, meaning Y2K is big and bad but we weather the deluge of failures and only the systematically weak are left with permanent damage. This is the Nietzschean social scenario that says, *that which does not collectively kill us, makes us collectively stronger*. Humanity emerges on the far side of this crisis with a renewed confidence vis-a-vis the invisible and pervasive information technology that seems to control so much of our lives.
- *"Houston, We Have a Problem"* refers to the Next Worse Case Scenario, meaning Y2K comes in bits and pieces but we are surprised to realize how fragile our systems are. Like the Apollo 13 mission from which this quote was drawn, it seems as though relatively minor weaknesses—the IT-equivalent of an *Achilles' heel*—sequentially disable many sectors of society with ferocity, leading to cascading failures that can threaten the sum of the whole. Humanity emerges on the far side of this crisis split into winners and losers, meaning—respectively—those who proved resilient and those whose weaknesses were exposed. In some ways, Y2K will unfold something like a computer virus: those with sufficient immunity will survive just fine, while those with weakened immune systems will suffer catastrophically.
- *"Y2 KO!"* refers to the Worst Case Scenario, meaning Y2K is big and bad and we're far more vulnerable than we realized. We are collectively "knocked to the mat," with the real uncertainty being, do we get back up before the "referee" finishes his "count?" Or do we lie there prostrate, dazed and confused? Of course, at some point we do get up, and how humanity emerges on the far side of this crisis is largely determined by the nature of the "knockout." Is Y2K merely a "TKO," meaning a "knockout" attributed solely to "technical" failures? Or is Y2K a genuine "whupping" where all our systems (political, economic, social, and network) fail us miserably? In other words, are we merely embarrassed and so continue on as before? Or are we truly humbled and thus serious changes result?



Slide 10: Outcome Scenarios Arrayed by Y2K Onset Models

## Potential Y2K Impact by Country Groups: Conventional Wisdom Has Changed Over Time

The conventional wisdom on which countries around the world are more vulnerable to Y2K has changed dramatically over the past year. We display our interpretation of this changing debate in the following two slides.

First, a word on how we break down the world into four IT categories:

- We define an "Ultra-Modern" IT category as including only the United States, which, by all measures, stands head and shoulders above the rest of the planet in terms of IT adoption rates. To put it bluntly, there's no way Y2K will be bad enough to derail the U.S.'s progressive adoption of IT. There's simply no going back.
- A "Modern" IT category basically captures the rest of the OECD-type states (Organization for Economic Cooperation and Development) such as Japan, Germany, France, etc. These economies tend to be relatively distributed in terms of networks, but not nearly as "New Economy" in outlook or practice as the U.S. Like

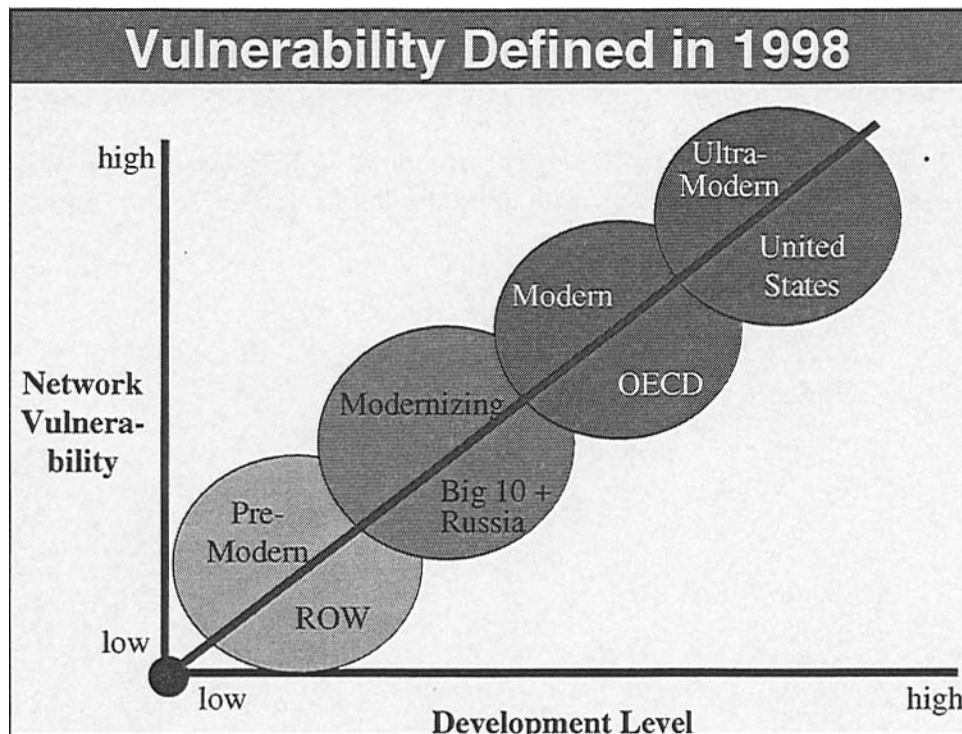
the U.S., these countries are unlikely to see the further adoption of IT derailed by Y2K, although it could greatly influence some of the choices they make in coming years.

- The "Modernizing" IT category corresponds to Jeffrey Garten's list of the "Big Ten" emerging economies, with the addition of Russia. Garten's "Big Ten" are:
  - China
  - India
  - Indonesia
  - South Korea
  - Turkey
  - South Africa
  - Poland
  - Mexico
  - Argentina
  - Brazil.

What's most immediately noticeable about this group is that you're talking about the bulk of the world's population, not to mention several that recently experienced serious economic tumult (or at least serious buffeting) in the Global Financial Crisis of 1997-98. With this group, you're also talking about countries that have adopted IT in a huge way only in the past decade or so, so Y2K has some potential here to trigger a bit of a technology backlash if its overall impact is bad enough.

- The "Pre-Modern" IT category bundles up the Rest of the World (ROW). Here we're talking about countries with low IT penetration rates.

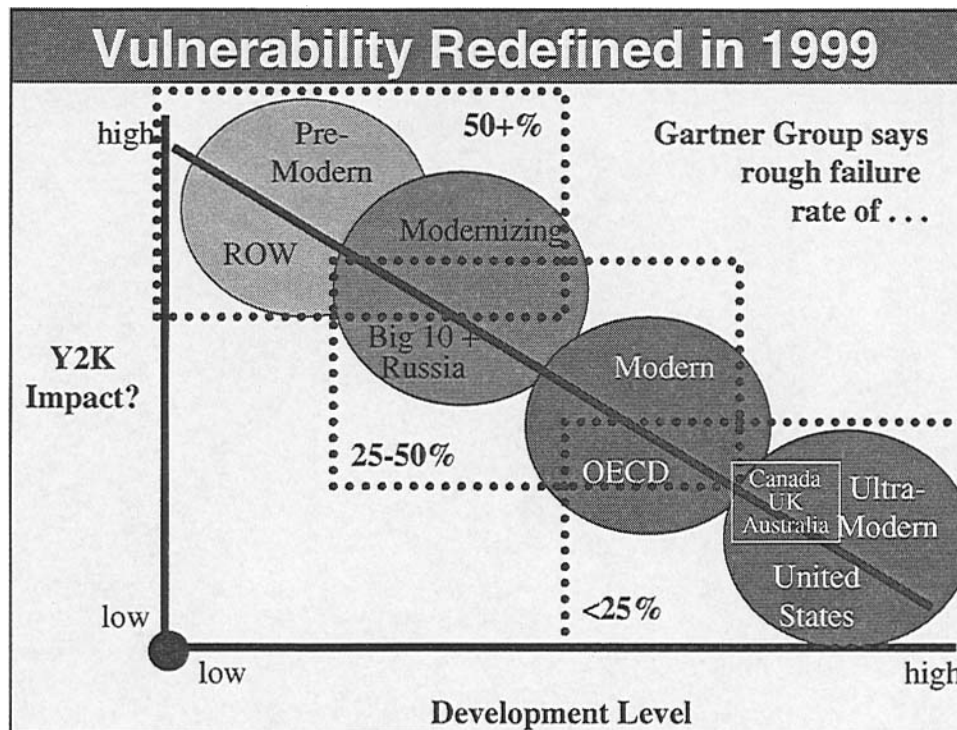
Slide 11 displays the conventional wisdom that we consistently bumped into when we began our research back in the summer of 1998. In short, the broad assumption implicit in most writings about Y2K's potential impact was that there was a direct relationship between a country's development level and its potential vulnerability on Y2K-induced network instability. Following this rule, an ultra-modern IT country like the U.S. was the most vulnerable, while Pre-Moderns like a Haiti or Somalia were least vulnerable. On the face of it, this made perfect sense, because you can't be harmed by breakdowns in what you don't have—or so it seemed. This thinking likewise tracked with much military strategizing regarding Information Warfare, which also posited that the more IT-intensive your society was, the more vulnerable it was to Information Warfare.



**Slide 11: Conventional Wisdom on Potential Y2K Impact (1998)**

What a difference a year makes! Or so it seems if you buy into the Gartner Group's estimates of likely Y2K network failure rates by country (see Slide 12). Now everyone knows that the Gartner Group's data is heavily based on the self reporting of the countries in question (or the private firms within those countries), so taking this very rough estimate with a grain of salt, you're nonetheless faced with a stunning reversal of fortune that's apparently occurred solely on the basis of the remediation efforts each country has or has not pursued over the last year. In short, from the perspective of failure rates, the U.S. goes from most vulnerable to least vulnerable, along with a host of like-minded states (e.g., Canada, United Kingdom, Australia). On the other end of the spectrum, the countries looking at the highest failure rates are the modernizing countries, such as China and Russia, and the IT Pre-Moderns, such as Vietnam and Zimbabwe.

While failure rates (the percentage of system failures) are expected to be much higher in the pre-modern and modernizing countries than they are in the U.S. or OECD nations, failure rates do not, by themselves, describe the whole picture. As noted earlier, IT is far more integrated into the economies and infrastructure of modern countries than those of emerging and modernizing nations are. Consequentially, 25 percent system failure in the U.S. is likely to be much more significant than a 90 percent failure in a small pre-modern nation. In the most primitive of these, even 100 percent system failure is likely to be below the event horizon; while even 10 percent system failure in a modern IT-intensive economy could result in significant economic upheaval. As suggested in Slide 13, when

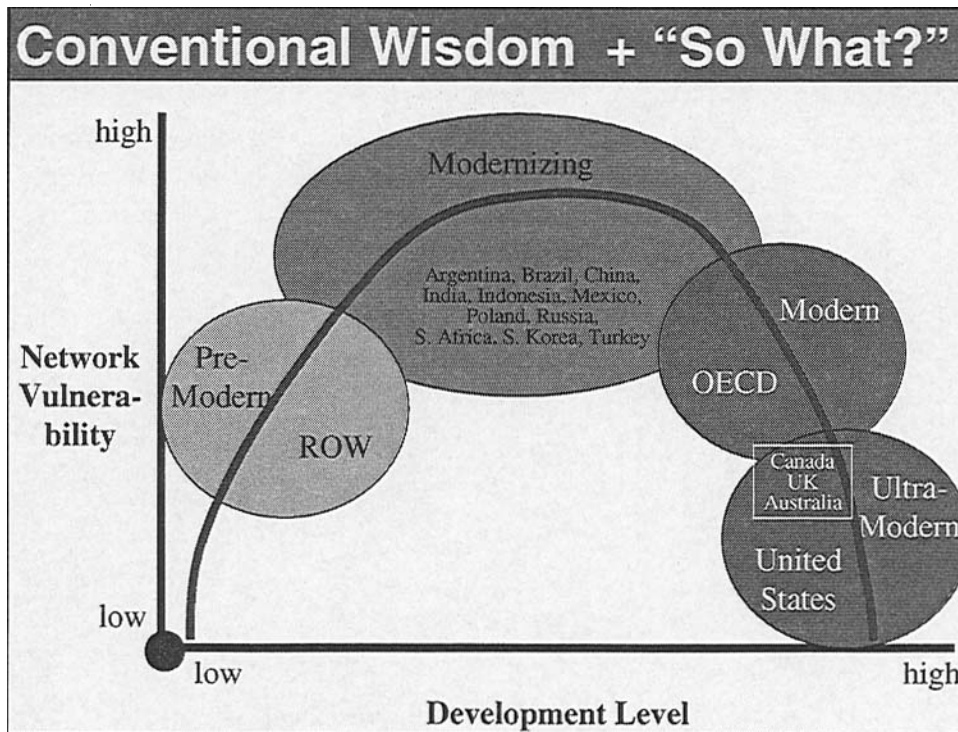


Slide 12: Conventional Wisdom on Potential Y2K Impact (1999)

all the factors—remediation effort, dependency on IT, network maturity, distribution and redundancy of the architecture—are integrated, the nations that seem to have the most to fear from Y2K would seem to be those in the process of modernizing. In general these tend to be increasingly dependent on IT, but have not been able to spend much money on remediation and have not developed the highly distributed and redundant networks of the U.S. and other modern nations.

So really, in the short span of about 12 months, the conventional wisdom on which countries are most vulnerable to Y2K has been dramatically reversed. Like the original conventional wisdom before 1999, this one also makes eminent sense when you think about it: rich countries with a lot more to lose and a lot more disposable income to throw at the problem have succeeded most in remediating the Y2K threat into something more manageable. Meanwhile, countries new to the IT scene, whose awareness of Y2K lagged significantly behind that of more advanced IT countries, tend to possess less resources to throw at the problem. Moreover, they tend to pirate software more and, as such, pay less attention to system administration concerns such as Y2K or viruses such as CIH. In that sense, the destructive path of CIH, the so-called Chernobyl virus, may well prove to be reasonably predictive of Y2K's ultimate impact—namely, more serious in Asia, Latin America, and the Middle East than in Europe or North America.



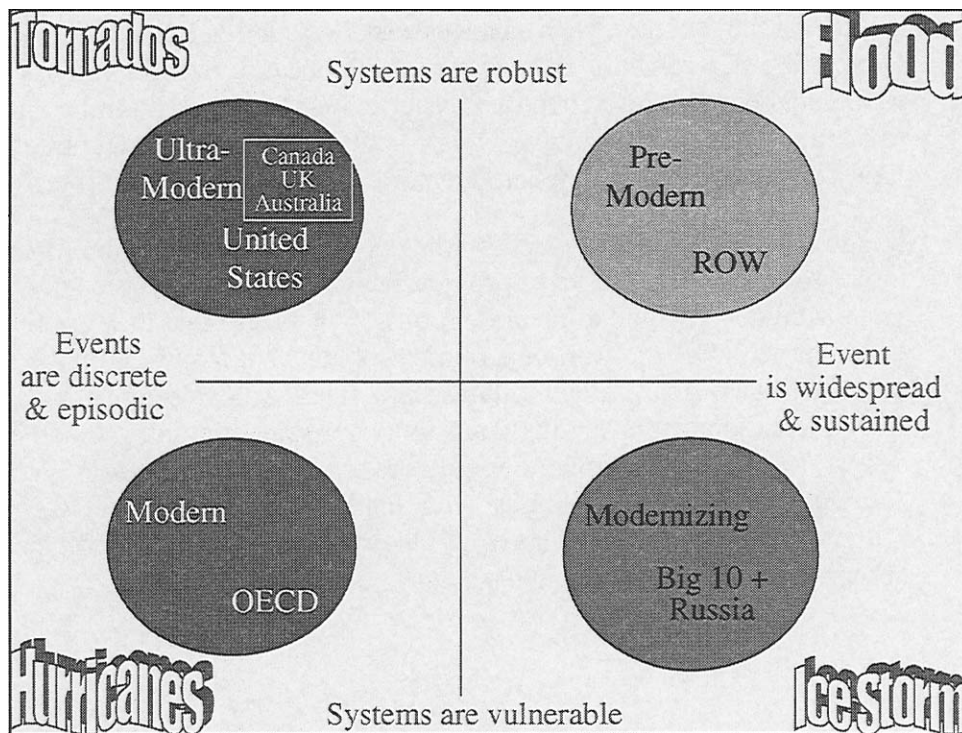


**Slide 13: So-What Filter Applied to Conventional Wisdom on Country Vulnerability**

## Matching Country Groups With Y2K Onset Models

So, to the extent that we're willing to go out on a limb regarding which country groups are likely to experience which Y2K onset model, our best guess would be as portrayed in Slide 14.

By arraying the countries across our X-Y axis, we're not so much predicting how we think Y2K will unfold for each and every country belonging to each grouping as suggesting that if any one of the onset models is going to be strongly associated with a particular development or IT-intensiveness level, they are likely to correspond as follows:



**Slide 14: How Y2K May Go Down By Country Groupings**

- We see the U.S., along with very similarly structured near Ultra-Modern states such as Canada, Australia, and UK, probably experiencing the *Tornadoes* onset model, meaning that Y2K comes in bits and pieces and the countries are essentially robust. Gartner predicts several other advanced European states, along with Israel, will fall into this category. Correspondingly, this country group would likely experience the outcome scenario described as *Run of the "Mille."*
- To the extent that many important Modern states, such as France, Germany, Italy and Japan, have not progressed nearly as much as they might have in the time allotted, we expect that this country grouping may experience something closer to the *Hurricanes* onset model. In short, we see the damage stemming from Y2K failures to be more significant than it might have needed to be because those countries enter into the situation more vulnerable than they realize. Correspondingly, this country group would likely experience the outcome scenario described as *Houston, We Have a Problem.*

- If the *Ice Storm* model actually occurs, we believe it's most likely to happen to a Modernizing country, such as a Russia, China, India, Poland, or Turkey. Here, Y2K may hit with far more force both because remediation has been weak and because these countries' systems are—in general—more vulnerable to disruptions. Correspondingly, this country group would therefore be more likely to experience the outcome scenario described as *Y2 KO!*.
  - It is in the IT Pre-Modern category that we expect to witness the *Flood* onset model, or the slow build-up of progressive failures. While these countries' systems in general tend to be more robust in the sense that they are more used to "doing without" or "working around problems," it may well be the slow but steady deluge of many small failures that causes Y2K to seem like a widespread and sustained event that drags out over several months. Good candidates for *Flood* status would therefore be less developed states in Latin America, Africa, the Middle East, and South and Southeast Asia. Correspondingly, this country group would likely experience the outcome scenario described as *Humans 1, Computers 0*.
-

## IV. The M Curve of Influence

### Understanding Where Opinion Leaders Can Influence Social Response

The strategic vision of Y2K we have encountered again and again, both in our Internet-based research and in our many discussions with experts and ordinary citizens from around the world, is that the event will unfold, peak, and then disappear—all with great speed—in a tight timeline surrounding the Millennial Date Change Event. In effect, what the majority expects is a very tall Bell Curve surrounding 010100, which we depict in Slide 15.

In other words, the conventional expectation is that Y2K failures will:

- Ramp up dramatically along an asymptotic curve in the last couple of months in 1999
- Experience a rapid topping off in the first few days of 2000
- Decrease in a similarly steeped downward curve until basically disappearing as a phenomenon of note somewhere in the middle of the First Quarter of 2000.

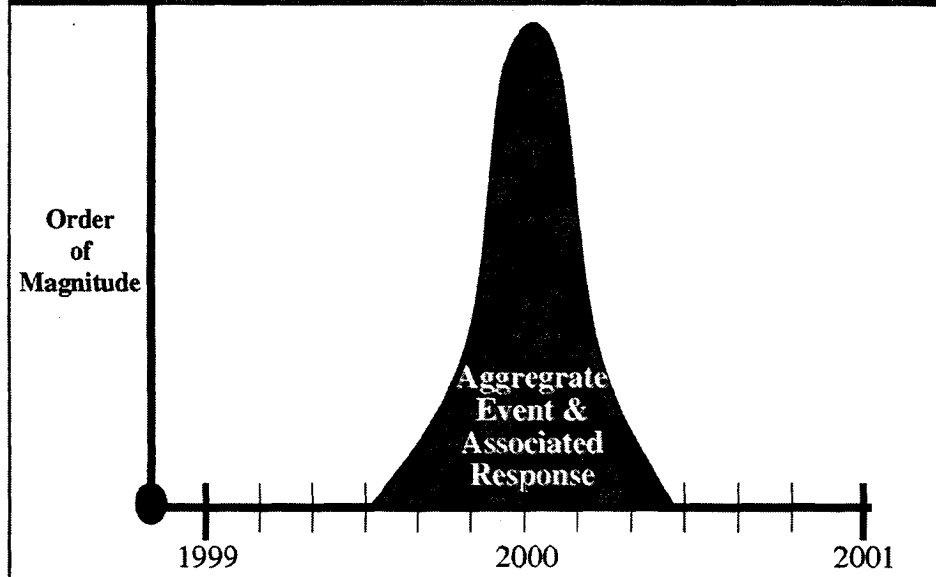
The problem with this view is three-fold:

- It tends to draw off strategic resources from both mid-1999 and the rest of year 2000 (and beyond) and concentrates crisis management approaches on the 010100 threshold.
- It inaccurately reflects the likely spread of Y2K-related network failures, as predicted by the Gartner Group.
- It fools decision-makers into thinking that not only will their influence be best used in a concentrated fashion around the 010100 threshold, but that it will likewise be effective during that specific period.

We believe one or more of these three mistaken assumptions are incorporated—to some degree—in much if not all of the strategic planning for crisis management of the Y2K Event around the world.

Instead of focusing on a Bell Curve perspective regarding Y2K's onset and unfolding, we argue that Opinion Leaders, whom we'll define as anyone with the power to influence the

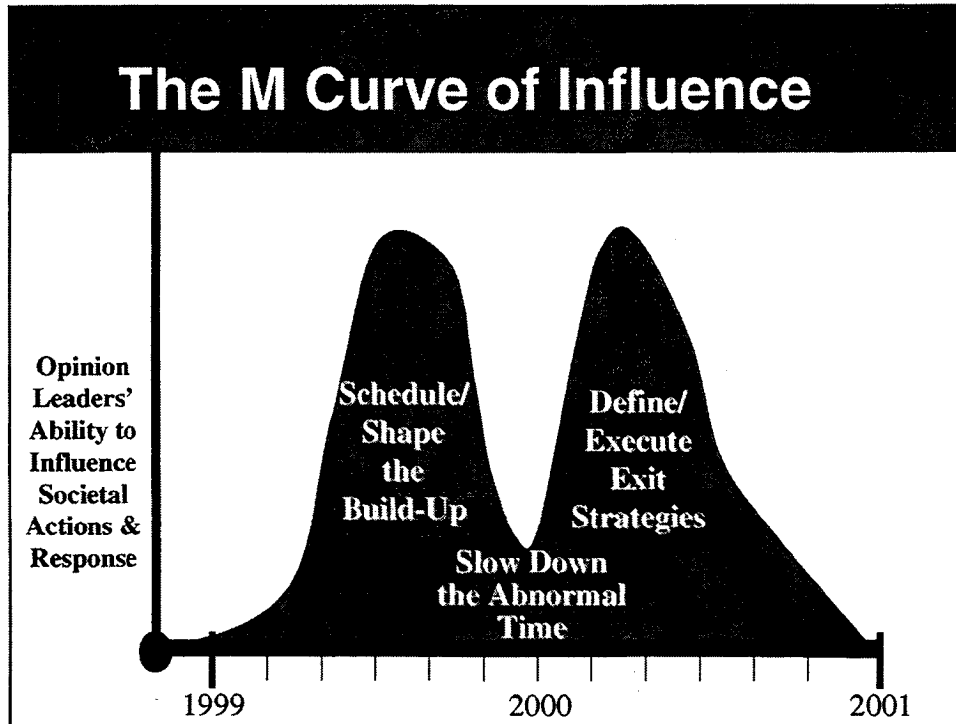
## Presumed Y2K “Bell Curve”



Slide 15: The Y2K Bell Curve Too Many People Expect

actions of others, should instead approach the Y2K timeline with the following three assumptions in tow:

- Your best time to influence social response is during the months leading up to Y2K's onset, with an emphasis on reasonable mass preparations, the establishment of crisis management arrangements, and the shaping of popular perceptions as to what will likely lie ahead.
- Your influence will disappear in the last few weeks and days leading up to the 010100 threshold, as the public will have largely made up its mind regarding individual preparations and strategies for experiencing—not to mention celebrating—the Millennial Date Change Event and the associated onset of Y2K; moreover, your influence will never be lower than on 010100, when your ability to control mass events will essentially approach zero.
- Your influence will reemerge once the Millennial Date Change Event expires and the true nature of Y2K's unfolding—however bad or minor that may be—makes itself apparent to you and society, for at that point you will have problems to solve, targets for resource allocation, etc.—in short, the battle will be joined.



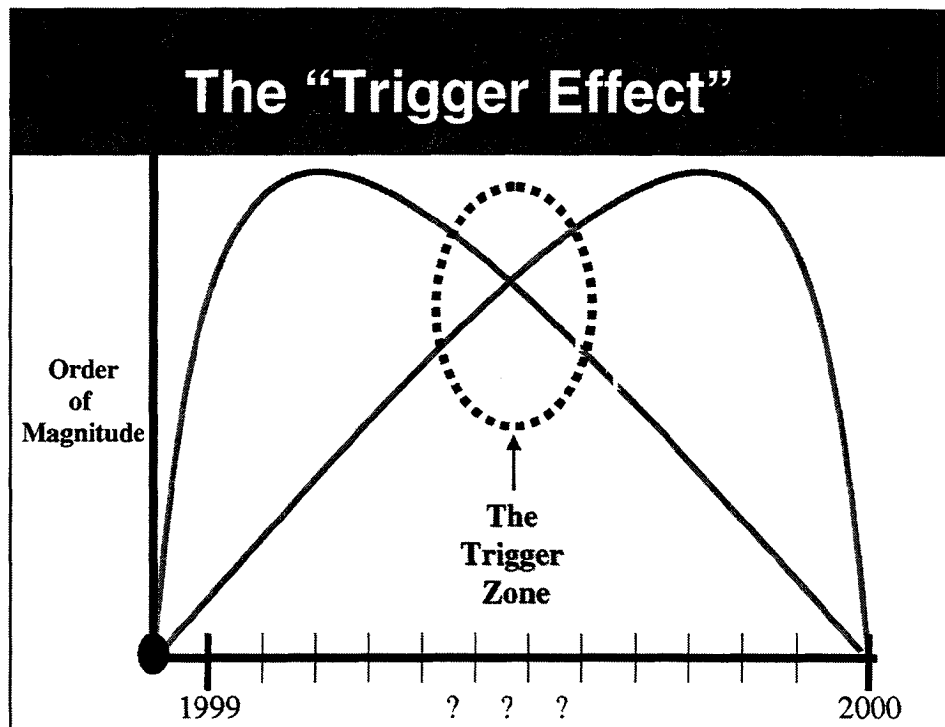
Slide 16: The M Curve of Influence Explained

Thus our "M Curve of Influence" (Slide 16) describes both the utility of Opinion Leaders' efforts before (*Schedule/Shape the Build-Up*) and after (*Define/Execute Exit Strategies*) Y2K's onset, while emphasizing the loss of influence over societal actions and response during the actual onset (*Slow Down the Abnormal Time*). In short, our strategic advice mantra would be:

***Organize . . . Relax . . . Attack***

## Explaining the First, or Pre-010100 "Hump" of the M Curve

We ascribe the first hump of the M Curve, or the bulge of influence we think Opinion Leaders enjoy over the summer and fall of 1999, to what we describe as the popular competition between *awareness* and *fear* regarding Y2K and the associated Millennial Date Change Event. Slide 17 explains this competition.



Slide 17: The "Trigger Effect" Explained

The first thing to note on the slide is our humility. The vertical axis is labeled "Order of Magnitude," which is just a fancy way of saying we're theorizing about a very complex phenomenon and thus can only describe it in rather vague terms. The timeline, on the other hand, is fairly straightforward—namely, we're talking about 1999.

It's our general hypothesis that no matter what country you're talking about, awareness of Y2K will precede—and in some ways, trigger—fear about Y2K. In a generic situation, then, we're describing the rise of "Awareness and the Public Transcript" as occurring more in the first half of 1999 than in the second half, meaning most people heard and came to understand Y2K in the initial sense in early 1999. This happened primarily as a result of their being flooded with all sorts of Public Transcripts about the state of remediation efforts and the (typically) non-likelihood of Y2K-related failures come 010100. Public Transcripts can be described as authoritative statements by authoritative people. They typically highlight a rosier-than-average perspective on Y2K, quite often out of official fear of "alarming the public unnecessarily." Of course, much of the awareness-raising effort encapsulated in such Public Transcripts requires "scaring" the public enough to take action, and therein lies the rub.

As we enter into the summer and fall of 1999, the Awareness and Public Transcript wave begins to give way (i.e., awareness has peaked) to the Fear and Private Transcript wave,

which is likely to peak in the last few weeks and days of the year. The fear part of the equation is nothing more than anxiety over the uncertainty caused by the looming event, whereas the Private Transcript describes the "off-line," unofficial, or individual preparations and/or decision making regarding how a person, economic firm, national government, etc., plans on either enacting or following a particular rule set for what it perceives will be the crisis period surrounding Y2K. So, for example, the differences between a Public and Private Transcript could be as follows:

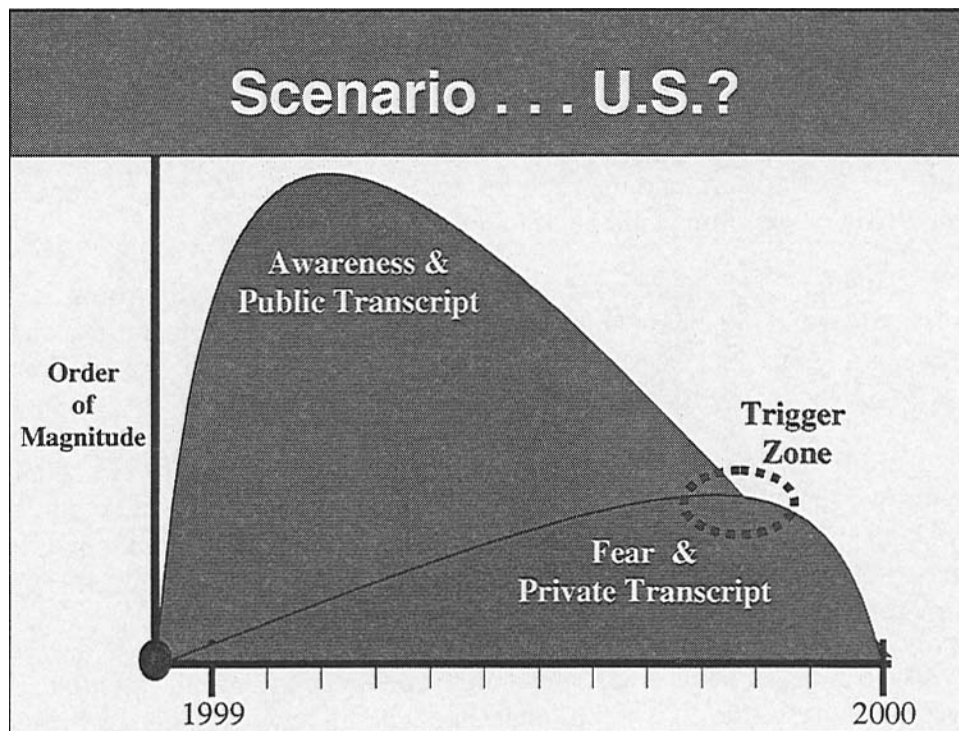
- An individual's Public Transcript could be that he or she is administrator of a small town and thus plays a prominent role in community preparations and perception management while simultaneously engaging in the Private Transcript of stockpiling food, water, and weapons at home.
- A firm's Public Transcript could be publicizing the success of its remediation effort while its Private Transcript could be its quiet stockpiling of key industrial material inputs, the cutting of ties with suppliers and vendors it does not deem sufficiently compliant, or the preparation and public announcement of new rule sets.
- A government's Public Transcript could be publicizing how all essential services will survive the Y2K Event intact and without any disruptions while quietly establishing all sorts of emergency procedures to deal with just such failures.

We describe the point in the year when the Awareness and Public Transcript wave is surpassed by the Fear and Private Transcript wave as constituting a Trigger Zone of sorts. This is where we believe the manic, or Mania Phase of Y2K begins. In short, this is when you will see individuals, firms, and perhaps even governments start to exhibit extraordinary behavior in response to whatever they believe "others" in society may do—i.e., *the fear of fear itself*.

Having said all that, we want to be careful not to leave readers with the impression that we're predicting a serious "freak out" factor for the United States come Labor Day, for it is by no means a given that the Fear and Private Transcript must overwhelm the Awareness and Public Transcript wave. In effect, if Opinion Leaders do their job correctly in terms of the Awareness and Public Transcript effort, the Fear and Private Transcript wave can be greatly reduced (see Slide 18). By way of analogy, think of how Wall Street spent much of the 1990s educating Baby Boomers about the dangers of yanking their money out of mutual funds at the first sign of trouble. Then think about how well that effort paid off during the Global Financial Crisis of 1997-98. In short, the better Opinion Leaders shape popular expectations, the less likely it is that Fear and the Private Transcript will balloon to dangerous proportions—not *every knee has to jerk*.

And indeed, it is our impression that as far as the United States is concerned, it is quite possible that the Fear and Private Transcript wave will remain marginal, meaning perhaps 15 to 20 percent of the population will engage in fear-based behavior that could be de

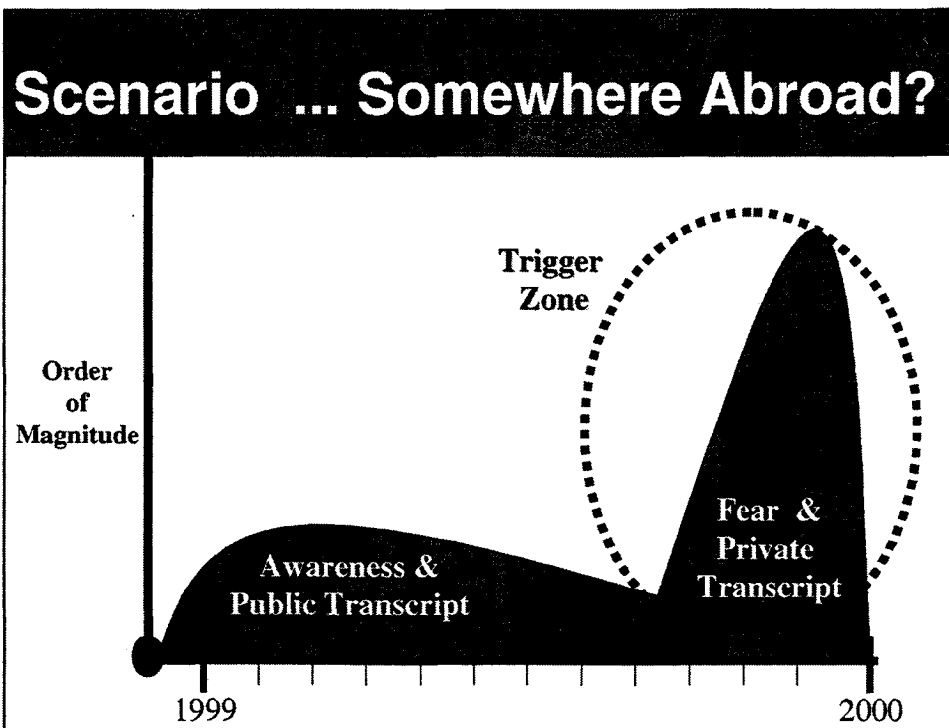




Slide 18: What the Trigger Zone Might Look Like in U.S.

scribed as "excessive," understanding what a loaded term that is for many in the Y2K debate.

When looking abroad, however, we are far less sanguine outside of Canada, Australia, the U.K., and a few other, mostly northern European states. In many countries overseas, we perceive the Awareness and Public Transcript effort to be woefully inadequate, thus inviting an explosion of the Fear and Private Transcript wave once the public comes to grasp what may be—by then—a significant and largely unavoidable period of profound network failures (see Slide 19). In this dynamic situation, Opinion Leaders in these countries will see their influence plummet and possibly be curtailed for a far greater time post-010100 than would have otherwise occurred, meaning a popular backlash.

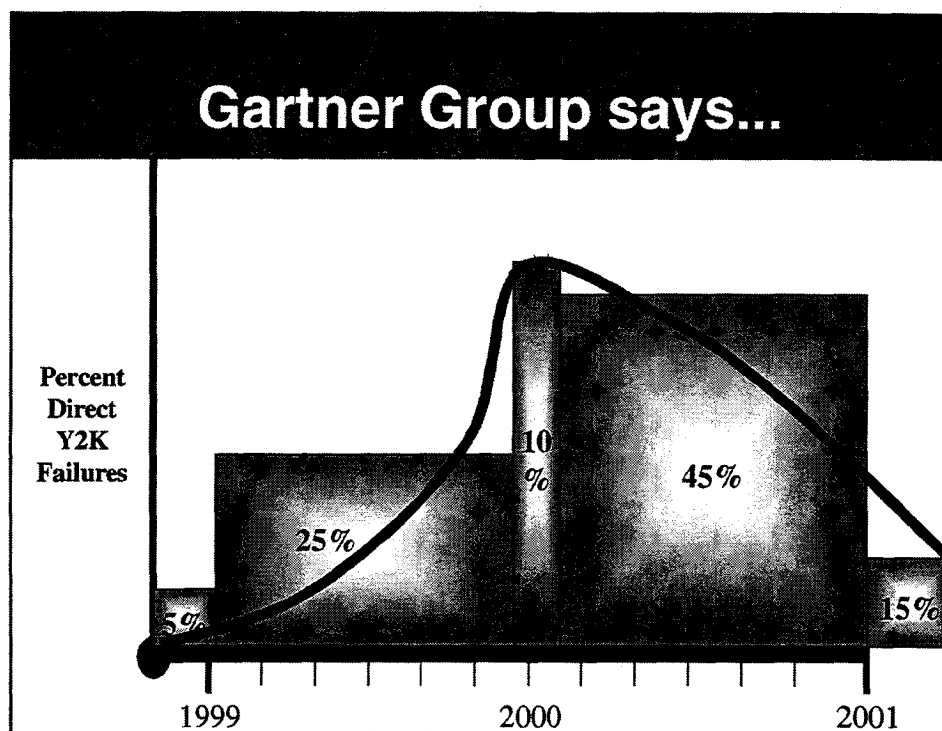


Slide 19: What the Trigger Zone Might Look Like Overseas

## Explaining the Second, or Post-010100 "Hump" of the M Curve

We ascribe the second hump of the M Curve to nothing more than the prediction by the Gartner Group that as much as 70 percent of Y2K failures will occur after 1 January 2000. As depicted in Slide 20, the Gartner Group estimates that only about one-third of all Y2K-related failures will have occurred by the end of 1999, leaving upwards of two-thirds or more still to unfold once the clock strikes midnight on 31 December 1999.

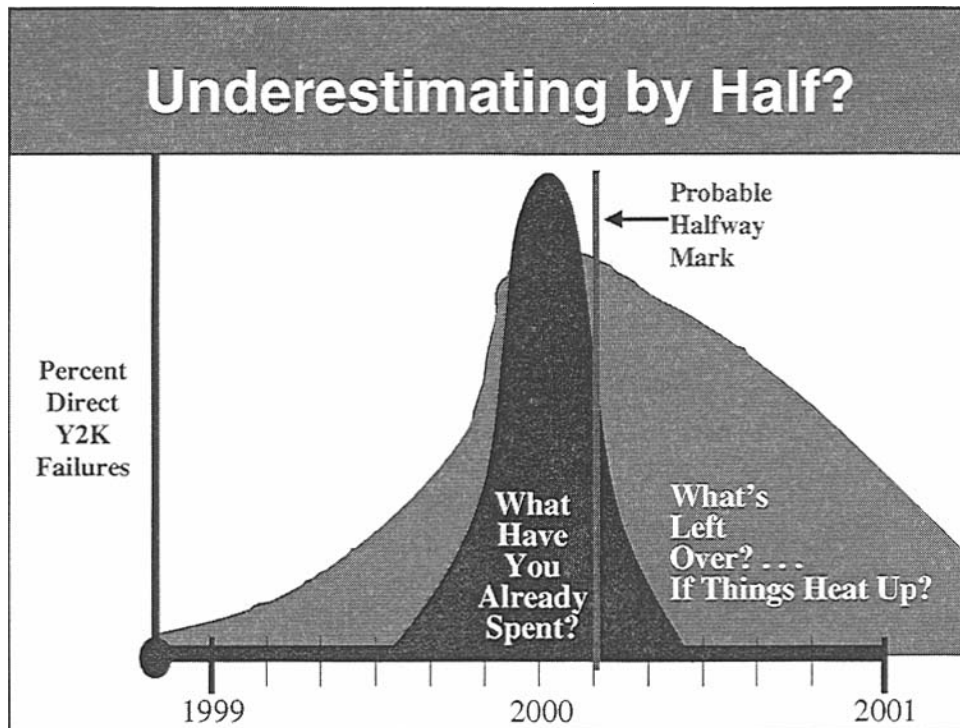
True to the Bell Curve image, Gartner is predicting that the highest frequency rate will occur in the ten days surrounding the 010100 threshold, where 10 percent of all Y2K failures will be concentrated. However, their prediction that close to two-thirds, or 60 percent of Y2K-related failures will follow this peak frequency period stands in dramatic contradiction of the Bell Curve assumption. Why we push the notion of the second, or post-010100 "hump" in the M Curve of Influence is our concern that too many decision makers in positions of authority will, in their concern for maintaining control over what we perceive will be a largely uncontrollable situation surrounding the Millennial Date



Slide 20: The Gartner Group Prediction on Y2K Failure Rates

Change Event, squander precious resources that should be held in reserve for the failures yet to come.

Another way to express our general concern is to raise the following issue, portrayed in Slide 21. If the halfway point in Y2K-related failures doesn't occur until some point *after* both the Millennial Date Change Event *and* the peak frequency period of 10 days surrounding the 010100 threshold, then what is the danger that private and public organizations will have misallocated their resources based on a predicted disruption period lasting through only the first few days of January 2000? Note, we're not saying to abandon such predictions or weather analogies (such as the Three-Day Snowstorm analogy), because most are based on the predicted loss of utilities—primarily electricity. For that particular core set of issues, the *days-long* predictions as an expectation management tool may well be appropriate. However, for other aspects of the economy, the *days-long* paradigm may end up misleading and thus misdirecting the strategic use of resources, not because individual disruptions last longer than a few days, but because the cumulative period wherein many simultaneous days-long disruptions occur may drag on for weeks or even months in certain countries.

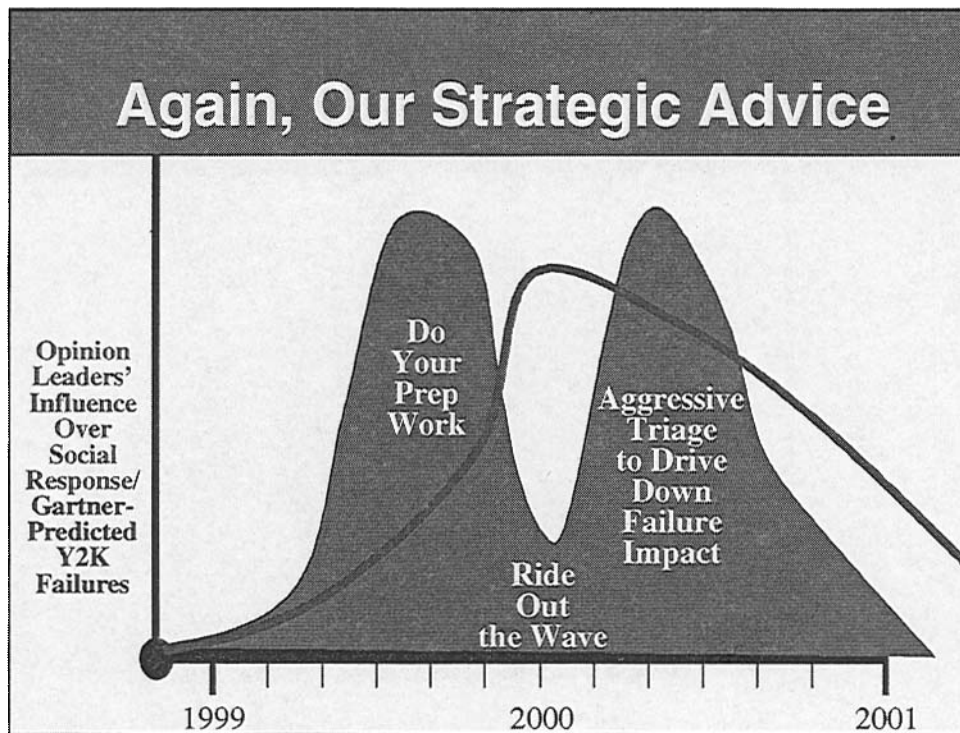


Slide 21: The Gartner Curve Versus the Bell Curve

## Summing Up Our Strategic Advice From The M Curve

Slide 22 juxtaposes the M Curve of Influence against the Gartner Group's curve of Y2K-related failure rates. By presenting both projections together, we seek to highlight what may—at first glance—seem like the counterintuitive nature of our strategic advice.

To sum up: we believe Opinion Leaders should concentrate their strategic resources and efforts at two distinct points in the Y2K Event timeline—namely, during the pre-010100 and post-010100 phases. Correspondingly, we think it best not to try to exert too much social control or direction during the Millennial Date Change Event or Y2K's immediate onset surrounding the 010100 threshold. Much like in preparing for the landfall of a hurricane, we think authorities should concentrate their activities in the following three-pronged manner:



Slide 22: The Gartner Curve Versus the M Curve of Influence

- Prior to 010100, do as much as you can to prepare the population for inevitable disruptions, with a strong emphasis on shaping expectations and delineating personal crisis management strategies.
- When the 010100 threshold looms and then passes, do not try to control events that cannot be controlled, but seek to "ride out the wave."
- Past the initial wave of high-frequency failures, engage in aggressive triage to drive down the impact of the remaining failures as they continue to unfold.

Our underlying philosophy in all of this advice is that *people in general respond quite well DURING disasters or crises, but that the panic potential beforehand and the "battle fatigue" danger afterwards are far more important management points than the actual threshold event.*

## V. The Scenario Dynamics Grid

### Creating a Composite, "Black Box" Scenario

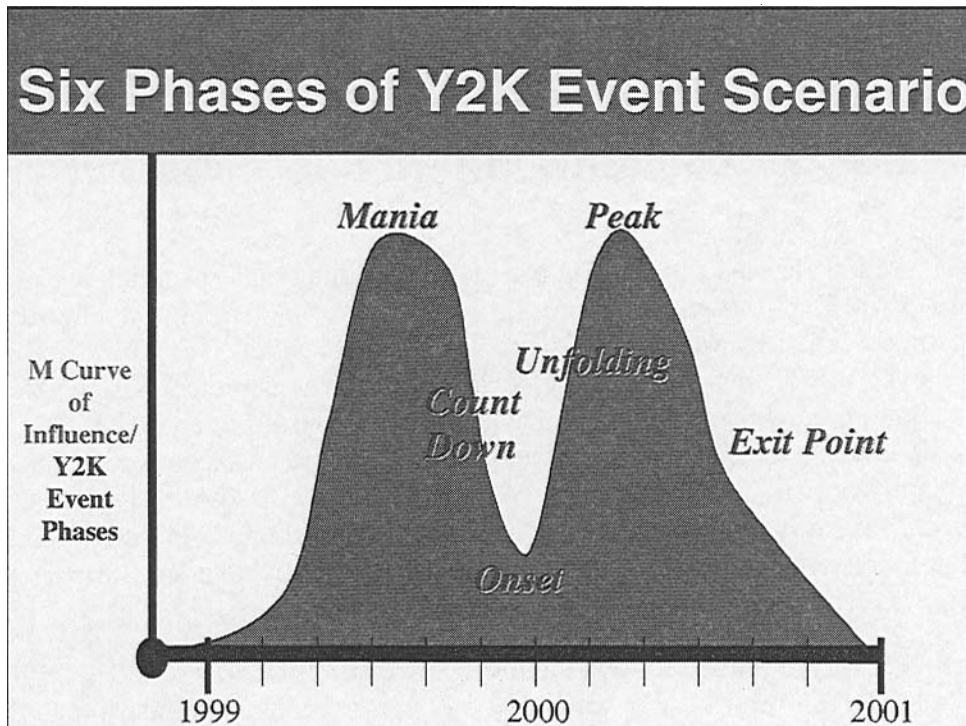
So far we've offered a series of "going in" and "coming out" scenarios for Y2K, with the Onset Models (*Tornados, Hurricanes, Flood, Ice Storm*) serving as the former and the Outcome Scenarios (*Run of the "Mille," Humans 1 Computers 0, Houston We Have a Problem, Y2 KO!*) serving as the latter. Again, we've constructed these bookend scenario sets less to predict than to frame the potential problem set presented by Y2K. In this section we'll tackle the "black box" in-between those bookend scenario sets, but rather than mechanistically trace *Best Case Onset Model* to *Best Case Event Scenario* to *Best Case Outcome Scenario* and so on, we're going to present a single composite scenario that is both phased and broken down into components sectors (Networks, Business, Social Response, Governance).

When we say "composite," we mean a single scenario that posits Y2K as both substantial and relatively drawn out. We won't offer any more detailed parameters than that, because we're not interested in debating those fine points that we can't really predict, but rather concentrate our analysis on the scenario dynamics we feel confident would appear in a reasonably stressing scenario. Having said that, we need to stress that this composite scenario is simultaneously about all countries and no one country in particular, meaning we strive for relatively generic content. Obviously, being Americans, our cultural biases will show through, but since we're writing first and foremost for U.S. decision makers, that's not the worst sin we could commit here.

By "composite" we also mean that no one should view this compilation of scenario dynamics as an all-or-nothing prediction (i.e., either we're right or we're wrong), for we don't think Y2K will go down exactly and completely like our scenario anywhere in the world. However, we do believe that many if not most of these dynamics will appear in a country suffering a dramatic Y2K experience, and we think that all of these dynamics will appear in some countries in various subsets and combinations. In short, this composite scenario should be viewed as a smorgasbord—i.e., *all of these items will be laid out on the Y2K table, but not every guest will partake of every dish.*

### Breaking Down the M Curve Into a Six-Phase Composite Scenario

Slide 23 breaks down the M Curve into six separate phases along a composite *stressing*



Slide 23: The Six Phase Composite Scenario Arrayed Against M Curve of Influence

Y2K scenario. We emphasize *stressing* because, if Y2K turned out to be a complete dud, then our M Curve of Influence would immediately go from being a Bactrian to a dromedary, or from a "two-hump" to a "one-hump camel."

As you view Slide 23 and read the explanation below, *please keep in mind that the M Curve does not represent the course of Y2K failure rates, but only our sense of the peaks and valleys of Opinion Leaders' capacity to influence social responses to such failures.*

We explain the six separate phases as follows:

**Mania** refers to the phase during which public awareness, anxiety, and preparation for Y2K accelerates dramatically. For most countries, this will be across the summer and/or fall of 1999, with the "size" of the mania growing in direct relationship with the lateness of its onset (meaning the later in the year it starts, the more profound it will be). For the U.S., for example, we'd predict the Mania Phase to really kick in come Labor Day (i.e., end of summer and beginning of fall, when thoughts turn to preparing for the winter), but for a country like Russia, probably not until November.

In general, a good rule on start dates would seem to be: *the more "crises" a country has on its plate, the later will be the start of the Mania Phase*. Of course, if there's enough crises a country may well skip the entire concept for all the obvious reasons, but that would clearly be a special case outside of our generic model. One key assumption of this phase is that enough "evidence" (a very slippery concept here) surfaces by this time that says Y2K may well be significant *and/or* sufficient "public outcry" or "alarm" is orchestrated by Opinion Leaders (whether they come from officialdom or the public itself) to fuel the Mania in the absence of such "evidence."

There are probably several factors that will determine the intensity of the Mania phase. The first is the degree of obfuscation or denial associated with the Public Transcript. This can have two affects on the resulting mania:

- In cases where there is significant obfuscation/denial associated with the Public Transcript, once the Private Transcript (perceived truth) is revealed, there is likely to be a very large delta between the public and private positions (i.e., between what I'm told and what I see). The degree of discontinuity between the two positions is likely to be one of the primary determinants of mania intensity.
- The greater the obfuscation in the Public Transcript, the more evidence to the contrary (Private Transcript) will have to emerge before the public script is rejected by the masses. This might very well delay the emergence of the widespread concern until very late in the game.

This brings us to the second primary determinants of mania intensity, *available preparation time*. The later in the game the Private Transcript is revealed, the greater the Mania is likely to be for any particular delta between Public and Private transcripts. The Mania is most accentuated when large public vs. private discontinuities appear so late in the year that people feel they no longer have adequate time to prepare for an event that now seems will be very different from what they've been told to expect. Here we'd see the increased likelihood of shortages, panic, and generalized iatrogenic activity.

The third important factor is mass trust in the ruling elites. If you believe in your leader strongly enough, you'll follow him or her right into a brick wall (or a spaceship hiding behind a comet). In extreme cases, trust in leadership could completely dissipate the mania. Of course, if the leader is overly optimistic, the Onset and Unfolding phases could provide a rude awakening.

Ultimately, frequent communication between the leader and the led, along with the most transparent possible information on Y2K preparations, seem to provide the best opportunity to mitigate the Mania.

**Countdown** refers to last few weeks and days of 1999, when individual and group preparation for the Y2K and associated Millennial Date Change Event takes on a life of its own, meaning the *simultaneous actions of a substantial portion of the populace rapidly propels Y2K up to the level of a social phenomenon no longer easily made subject to*



*any organizational control—private or public.* On the face of it, that sounds pretty scary, but depending on the society and culture, it need not be.

Much will depend on the individual's sense of vulnerability in the face of a potentially destabilizing event, and that sense of vulnerability will depend proximately on his or her sense of achieved preparations but ultimately on his or her expectation of the event ahead. Preparations alone are unlikely to reduce uncertainty, thus the previously shaped expectations of the public at large will loom large at this point. But like riders traversing the first great drop of a roller coaster ride, few minds are likely to be changed in transit. Most people will turn a blind eye and a deaf ear to further entreaties or advice, as they steel themselves for the remainder of the "ride."

***Onset*** refers to probably no more than the first week of January 2000, but is primarily concentrated on the 31 December 1999 (Friday) through 3 January 2000 (Monday) time frame. Y2K's overlap with the Millennial Date Change Event and all the associated angst, celebration, joy, and violence that milestone is likely to evoke from large numbers of people around the planet will make for a very confusing time period, during which far too many simultaneous local experiences will be processed for widespread consumption via a global mass media blow-out of epic proportions. Almost by definition, a crisis is a compression of time, during which "more things happen than usual," making societal response patterns unpredictable. So given all that's likely to be going on during Y2K's Onset Phase and the accompanying media saturation coverage, we will—by definition—experience a crisis atmosphere that will inevitably skew most people's perceptions of events.

***Unfolding*** refers to the indeterminate length of time (depending primarily on a country's level of IT) that will have to pass before the private and public leadership circles within individual countries can ascertain the extent of Y2K-induced network failures they collectively face. Our assumption here is that more advanced IT countries will more quickly catalogue and analyze those failure events that have already transpired and thus generate more accurate estimates of what's left to unfold than will less advanced IT countries.

As a crisis management rule, this capacity for gathering intelligence and processing estimates should not be considered a predictor for the country's aggregate failure rates, so a shorter Unfolding Phase shouldn't be considered commensurate with a less traumatic Y2K Event, for the rush of failures is likely to be greater and thus more traumatic in a shorter phase. However, in terms of social response dynamics, it's fair to assume that the shorter the Unfolding Phase, the easier it is for Opinion Leaders to rebuild their influence over public perceptions. Correspondingly, the longer the Unfolding Phase (meaning the longer the sense of public uncertainty regarding the question, "How bad will this whole thing turn to be?"), the greater the potential for mass iatrogenic behavior that only confuses the situation further and complicates both direct recovery and broader crisis management efforts.

***Peak*** refers to period during which a country experiences the maximum impact of its Y2K-induced network failures and whatever side effects those failures may create

throughout the economic, social and political arenas. Naturally, the definition of "peak" is highly subjective, since it is very unlikely that countries or regions will experience Y2K in a collective, unifying sense. Y2K, if it turns out to be substantial for any one country, is likely to exhibit a strong "localizing" effect, meaning it will tend to cut communities off from one another, thus varying their individual experiences greatly. As such, any attempts to define or declare—on a country-wide basis—the "peak" of the Y2K Event will be highly contentious and politicized affair.

**Exit Point** refers to either an apparent or a self-declared end to the systemic Y2K Event and any associated crises. Like the definition of the "peak," this will be a highly contentious and politicized debate that will—assuming Y2K has been substantial—*immediately* segue into, and thus set many of the key judgment parameters for, the official and unofficial "score settling" that inevitably accompanies any crisis period. For example, in the United States the Y2K Exit Point is likely to overlap with the first few weeks of the 2000 presidential primary season.

One key alternative scenario element for this phase is the emergence of a follow-on crisis—whether it be related or unrelated to Y2K—that effectively "ends" the Y2K Event by superseding it in national importance. Of course, in this instance, much would depend on the public's perception of the causality surrounding the "new crisis"—namely, did it truly arise "on its own" or was it "engineered" by "powers-that-be" to divert public attention from the continuing Y2K crisis (e.g., the "splendid little war" scenario, alternatively known as the "wag the dog" scenario).

## The Scenario Dynamic Grid Explained

Slide 24 presents our Y2K Scenario Dynamic Grid. The four-by-six grid is arrayed in the following manner:

- The four rows correspond to our four Y2K sector areas:
  - Networks
  - Business
  - Social Response
  - Governance.
- The six columns correspond to our six-phase composite scenario timeline:
  - Mania
  - Countdown

- Onset
  - Unfolding
  - Peak
  - Exit Point.
- The main entry for each grid box represents our definition of the key scenario dynamic in play for that sector area during that scenario phase. For example, "F2Q," or "flight to quality" is the key scenario dynamic in play in the Business sector during the Countdown Phase.
  - The secondary entry (in the smaller red box-arrows) for each grid box represents our definition of a key emerging scenario dynamic to look out for as the timeline moves from that particular phase to the next one. For example, "Answer Man" is the key emerging scenario dynamic to watch for as the timeline moves from the Unfolding Phase to the Peak Phase in the Governance sector.

We offer the same general caveat regarding the Scenario Dynamics Grid that we cited for the M Curve: we feel fairly confident that the first three phases (Mania, Countdown, and Onset) will occur regardless of how Y2K actually unfolds post-010100, so the dynamics we cite in those columns are essentially predictions that we think will come true in some combination for enough states around the world so as to serve as a useful generic model. As for the final three phases (Unfolding, Peak, Exit Point), there we're getting into hypotheses regarding an assumed Y2K Event that proves to be stressing and substantial. In that regard, the scenario dynamics listed for those columns do not represent predictions of what must happen—only estimates of what could happen given a particular stressing scenario. In other words, if Y2K is a dud, you can largely forget the last three columns.

## The Network Timeline in Detail

Moving from left to right along the timeline:

In the *Mania Phase* you see the ramping up of the ***Stockpiling*** dynamic, with individual stockpiling attracting the most media attention, even though it's the stockpiling by economic firms and governments that will have far more profound market impact. Of course, stockpiling will occur in direct relationship to public fears concerning the interruptions of key network services (utilities and food distribution being the big drivers), and will reflect the strategic distance between the Public and Private Transcripts of business firms, i.e., the difference between what they're saying to reassure customers and the steps they're taking to deal with non-compliant suppliers and vendors. In both instances (individual and organizational stockpiling), it's the "little guy" who will suffer or fall behind, thus increasing "his" anxiety.

	Mania	Count Down	Onset	Unfolding	Peak	Exit
2000-01-01	Stock-piling Most Vulnerable	Getting (It) There Going Offline	System Overload Black Outs	Rationing Traffic Jams	Haves vs Have Nots Network Leviathans	Metropolis Saved NEW FAULT LINES
2000-01-02	Taking Options Leper Lists	F2Q Cash on Hand	Dead Zone Market Quakes	Islanding/ Fortressing Personal GDP	Cash Economy SME Triage	Winners Crowned NEW RULES
2000-01-03	The Truth is Out There Rumor Mills	Info Overload Final Solutions	Will to Party Panic Release	Iatrogenic Zone Trigger Effect	Scape Goating Guilty Will Pay	"Worst is Over!" NEW FAITHS
2000-01-04	Credibility Gap Y2K & U	Authority On Tap First Strike	Keeping Up Appearance Opportunists Abound	Backlash Answer Man	Mobilization Capacity Killer Apps	Legal Decon-struction NEW RULERS

Slide 24: The Y2K Scenario Dynamics Grid

Thus the dynamic to watch as we go from *Mania* to *Countdown* is the emergence and increased agitation of the **Most Vulnerable**. On the individual basis, stockpiling is a middle-class (or better) phenomenon in that it requires disposable income that the poor do not possess. Since rural poor tend to have a better system of workarounds for these situations, the group to watch are the urban poor, who will likely be the first to feel any squeeze from stockpiling purchases and thus grow more anxious. In terms of economic firms, it's the Small/Medium Enterprises that will suffer, simply because they don't have the capital of larger firms to safeguard themselves against supplier disruptions.

In the *Countdown Phase*, **Getting (It) There** refers to two phenomena: 1) movement by people to locations where they may choose either to "celebrate" or "ride out" the millennial date-change event; and 2) a "topping off" of crucial supplies by individuals or organizations.

In the first sense, we expect to see a greater than average amount of travel in anticipation of the 010100-threshold. Rich people will want to travel somewhere exotic for fabulous celebrations. More religious-minded people will travel to holy meccas and shrines to celebrate Christendom's Third Millennium. Partygoers will pack urban areas for mammoth New Year's Eve extravaganzas. Apocalyptic-minded individuals will head to the

hills or sanctuaries. Safety-conscious people may leave urban areas for rural ones. Families may gather with even greater frequency, either out of a simple desire to share the moment or out of concern for more vulnerable members. Governments may organize and move around security and/or crisis management forces. In short, a lot of movement may occur, with gross numbers linked to popular anticipation of the event as being historic or "once in a lifetime."

The "topping off" phenomenon in Networks will occur along a myriad of avenues, with one good example being the advice proffered by many authorities that it would be wise for everyone to have their cars' gas tanks filled up. If, for example, a large majority of a population attempts to actualize that advice in the last 2 to 3 days on 1999, it is quite possible that spot shortages will immediately appear (i.e., gas lines) and most nations' distribution networks aren't set up to handle that much volume in a concentrated time period. This, of course, would create a social dynamic all its own.

As we move from *Countdown* to *Onset*, the dynamic to watch involves efforts by authorities to encourage both individuals and organizations to go off-line as much as possible in the last few hours of 1999 and during the first 24-72 hours of 2000 (i.e., through the holiday weekend). ***Going Off-line*** means doing whatever is possible to reduce loads on utility networks. For example, it means encouraging large-scale celebrations to be as low-tech as possible to reduce electricity loads. It may mean also that authorities encourage more distributed celebrations to reduce stress on mass transit networks. Much of any government's success in encouraging this conservation will depend greatly on previous public education campaigns. For example, in the U.S. the FCC has already begun asking the public not to use telephones or modems on 31 December and 1 January to avoid overloading the public telephone system. In effect, the FCC fears some combination of the "Mother's Day" effect (i.e., everyone calls family members to note the historic occasion) and a "testing the system" effect (i.e., everyone checking to see if the phones and Internet are still working). Of course, if everyone tests or calls Mom at the same time, the stress on the telephone network can become a self-fulfilled prophecy. In countries around the world with less robust public utility networks, this dynamic is all the more important.

A particular subset of the *Going Off-line* dynamic refers to the possibility that some energy power plants—namely nuclear power plants—may be taken off-line for some indeterminate period of time surrounding the 010100 threshold due primarily to safety concerns. If this were to happen, then obviously a country's energy power grid would suffer diminished load capacity. At this time, however, predictions regarding such actions are highly speculative. For example, earlier this year there was a lot of loose talk about airlines and ports shutting down for some period surrounding 010100, and although some isolated declarations of intent have been made (e.g., Virgin Airlines giving employees New Year's Day off for "family reasons"), widespread shutdowns in either industry seem ever more unlikely as time passes and confidence regarding Y2K grows.

Once we get to the *Onset Phase*, despite the best efforts by authorities to encourage low-voltage celebrations, we nonetheless foresee great potential for the overloading of network systems. Again, we're talking the world's largest party, plus it's the middle of winter

in the Northern Hemisphere. Factor in all the additional activity—and thus added network load—associated with Y2K, and we're looking at an inevitable spiking of demand for network services (e.g., electricity, phones, Internet access, mass transportation).

As such, it only makes sense as we move from *Onset* to *Unfolding* to watch out for **Black Outs**, or the disruptions of basic utilities, "downing" of the Internet in places, spotty phone service, etc. Current predictions for such disruptions range from the "Three-Day Snowstorm" analogy in the U.S. to predictions of far longer outages in places such as China or Russia. The key question for any country, though, is not whether the outages will happen, for some inevitably will, nor how long they last, as many countries deal quite nicely with such disruptions (thinking of Russia), but rather whether or not these blackouts represent the first of many interrelated waves of failures, or simply the early flame-out of the Y2K phenomenon.

If Y2K proves to be substantial and long-lasting, it will reveal itself in the *Unfolding Phase*, which in the Networks sector would lead to the dynamic of **Rationing**, meaning anything from rolling brownouts/blackouts in some utilities, to possible restrictions on access to mass transit or thoroughfares, to even the distribution of basic foodstuffs by authorities. The key point is that either non-market mechanisms will arise by government fiat and/or market prices will rise high enough to cause de facto rationing *by wealth* of items typically viewed as basic.

Since transportation of goods into areas where shortages exist is the primary means of relieving the rationing dynamic and thus ending the "localizing" phenomenon of Y2K-related network failures, it would be precisely a broad and continuing slowdown in this sector that would signal a movement from the *Unfolding* to *Peak Phase*—hence we cite the dynamic of **Traffic Jams** as the key indicator in this transition. A good example of the type of transportation slowdown would be the dozen or so global megaports through which flows the vast majority of goods shipped over the high seas. Substantial slowdown in several of these megaports would exacerbate the Y2K Event, with the most likely culprit in this equation being neither the ships themselves nor the off/on-loading networks, but rather the recording keeping—i.e., the paper work.

A *Peak Phase* in the Network sector would feature the dynamic of **Haves vs. Have Nots**, caused simply by the disparities in deprivation engendered by network failures. Reasons for this would include:

- Better preparations for deprivation by some
- More disposable resources for some to deal with deprivations once they appear
- Some areas will feature a higher percentage of vulnerable populations (e.g., very young, very old, sick or disabled)
- Localizing effect will mean some communities are better situated in terms of basic supplies than others (e.g., southern areas will be in growing season)

while northern areas will not)

- Remediation efforts will have varied greatly by area
- Failures will not be evenly distributed or evenly timed.

In short, because some people and/or areas will do better than others, tensions will inevitably rise between groups suffering varying levels of "pain" or varying rates of recovery. Note, this is not the same as saying "people tend to freak out" during disasters, for here we're past the initial "disaster" and deep into the painful aftermath. By analogy, the *Onset* would correspond to the "people coming together when disaster hits" notion, whereas the *Peak* corresponds to the period weeks later when tempers begin to flare as people start realizing that although "we were all in the same boat in the beginning," that initial leveling phenomenon has given way to serious differences in rates of recovery and the ultimate resumption of "life as we knew it."

Getting us from the *Peak* to *Exit Point*, which we define as *Metropolis Saved*, meaning that if the cities are back to near-normal then the crisis is largely over from a Network perspective, may require some extraordinary efforts by some extraordinary actors. These efforts must either solve the problem of "things not moving" by fixing the networks themselves or by generating and supporting sufficient workarounds to get things moving by alternative means. We have dubbed this dynamic *Network Leviathans*, meaning super-empowered organizations that can somehow make things move even when it seems that normal network pathways are hopelessly disabled. By definition, we're first and foremost talking about militaries here, for it's the military that specializes in creating logistical networks where none have previously existed—typically on a battlefield. The down side to this is that no military in the world comes even close to matching the logistic capabilities of the U.S. Military. The up side is that most militaries around the world have some real experience in providing these functions within their own countries during times of natural disasters. So if it's a ragged capability in many countries, at least it's one that's familiar. Given that the U.S. Military is unlikely to get deeply involved within the United States, given the relatively robust nature of our distributed police, emergency response, and National Guard networks, one of the main roles it may play will be that of *Network Leviathan* overseas in conjunction with international and foreign national relief organizations.

We end our discussion of the Network sector by positing the legacy issue of *New Faultlines*. By this we mean humanity discovering divisions among itself that were not apparent before the Y2K Event. In effect, we're talking about divisions based on information technology that have arisen during the past couple of decades but have not yet made themselves as obvious in a popular sense as they might be after a traumatic Y2K experience. The two obvious extremes of this equation are:

- Those "too dependent" on information technology will have their "comeuppance" while those more "self sufficient" will emerge from this experience

more confident about a future that inevitably features an ever increasingly frequency of this sort of IT "disaster."

- Those "too slow" on information technology will have their "comeuppance" while those who adapt themselves with greater speed will emerge from this experience more confident about a future that inevitably features an ever increasing IT quotient.

## The Business Timeline in Detail

Moving from left to right along the timeline:

In the *Mania Phase* we see the phenomenon of firms ***Taking Options***, meaning business firms setting up and/or implementing alternative supplier/vendor arrangements in anticipation that some portion of their existing supplier/vendor base will not perform well in the coming Y2K Event. This is a variant of life-as-we-are-coming-to-know-it in the New Economy, with its rapidly shifting alliance strategies and frequent market-share quakes, and yet, it may take on an added dimension here because of the (potential) simultaneous actions of many firms focused around a single date in time. But in the end, all it really says about business and finance is that when managers look ahead to Y2K, they see winners and losers, and therefore plan accordingly. Nothing personal, mind you, just business.

As we move from *Mania* to *Countdown*, a compelling dynamic becomes the appearance and use of ***Leper Lists***, which finger those suspected of not performing well in the coming Y2K Event. They are definitely a double-edged sword, for, on the one hand, they represent a great motivator for remediation laggards while, on the other hand, they can bring the same sort of self-fulfilling prophecies that one associates with rumors about a bank's liquidity—namely, bank runs. So if a supplier gets a bad wrap as "non-Y2K compliant" and then sees orders dry up as it is shunned by long-time business partners, then problems are bound to ensue regardless of the firm's ultimate Y2K vulnerability. The recent experience of the Global 2000 Coordinating Group and their near-publication of a Y2K-readiness rating of major trading nations (they backed off at the last minute for fear of sparking capital flight) speaks volumes about the dangers involved with such lists, and yet appear they will, for they represent serious intelligence about potential market failures by competitors. Firms will naturally want this information and—once they have it in hand—will naturally use it to their own advantage.

***Flight to Quality*** is the natural dynamic of choice for the *Countdown Phase*, for it speaks to the notions of last-minute panics and the desire for safe haven. Recent history has given us plenty of examples of what Thomas Friedman would call "stampeding" by the international "Electronic Herd" of global investors. Moreover, there's plenty of good history to back up the concern, as the *Economist* pointed out in its September 1998 survey of Y2K (19 September 1998, p. 4):



Since the start of modern times, the end of a century has been a time of economic unease. The British and Dutch stock markets in 1699 and 1799 and the Dow in 1899 all saw sharp falls in prices, according to ING Barings, a Dutch bank; between December 2nd and 18th 1899, the Dow fell by 23%. A millennium, even more than a centennial, would be spooky enough without the fear of computer failure. Perceptions, rather than reality, may turn out to be the most dangerous aspect of that pesky millennium bug.

Of course, none of this says anything about the mid-term stability of global financial markets, nor about Y2K, but only about the psychology of investors and their periodic tendency to engage in fear-fulfillment.

So where does the money go? Gold prices are at historical lows. The U.S. stock market is overvalued already by the measure of many experts, and yet would seem to offer a great place to park cash in the short run since the U.S. should come through Y2K okay. Or do Internet stocks come tumbling down, bearing the brunt of the technology fear? In short, you ask enough questions and fairly soon you're back in the life-as-we're-coming-to-know-it territory that one associates with the emerging New Economy, again begging the question of whether or not Y2K represents something fundamentally unique in history or a harbinger of the future.

The dynamic to watch as we move from *Countdown* to *Onset* is what we refer to as **Cash On Hand**, meaning both the issue of liquidity in markets (e.g., everyone trying to sell bonds at once in a certain small-country market and finding no buyers) and the issue of paper money in circulation. Both issues revolve around panic and the desire for fungible assets during a perceived time of great uncertainty. So cash on hand may be an important safety cushion for a country's central bank in terms of protecting themselves from both outside forces (e.g., foreign currency reserves to ward off speculators) and inside forces (e.g., sufficient money in circulation to ward off bank runs). A rule we might propose for this dynamic would be, the more control you have over your country's cash reserves (having more is obviously better) and money in circulation (to include the printing of money), the safer you are regarding Y2K-induced financial panics. Again, there's nothing terribly particular to Y2K about this advice, rather it's simply the occurrence of Y2K that highlights a capacity that countries are increasingly coming to value in a globalized New Economy.

With the *Onset* of Y2K, we expect to witness the dynamic of an economic **Dead Zone** that will encompass both retail and financial transactions. In retail, we're talking about a consumer that's already spent his or her available disposable income either on Y2K preparations or end/beginning-of-year holidays or some combination thereof. In the financial world, we're talking about companies—far more than usual—working to move transactions away from the end of the calendar year, meaning "earlier" into December or "later" into January. Again, neither of these dynamics is particular to Y2K or the Millennial Date Change Event, but are part of the normal end-of-calendar-year business cycle. All we're predicting here is a larger than normal effect. For example, we'd expect extra market "holidays" around the 010100 threshold in many countries around the world, as markets there attempt to ease their financial sectors past the date change in as relaxed fashion as possible (possibly phasing them in over several days before reaching full

working volume). Even if markets or governments didn't take these extraordinary steps, the wariness of individual firms and investors to play in those first few days might well do the trick all by itself.

Of course, at some point, financial markets have to come back online completely, and here's where our more speculative material kicks in. *If* Y2K turns out to be widespread and substantial in impact starting in January, the dynamic we look for in financial circles are what we'd call **Market Quakes**. This refers to Y2K-induced or related network failures that either directly disable financial market operations or create cascading investor panic about broader economic dynamics (including disabled market operations) that find their reflection in wild market swings. Such quakes, of course, can start anywhere on the planet, but once started, tend to move with time zones from one global super-market to another (e.g., from Tokyo to Hong Kong to Europe to London to New York and then all over again). Rather than labeling this dynamic a "financial contagion," it's really more a matter of copied behavior: investors in one market fear that what they're watching in another market is a clear indicator of their own future, thus eliciting similar defensive responses. For the business timeline as a whole, this is probably the key single dynamic, for if Y2K is going to kick into a larger economic downturn, the first real signs probably appear here. Conversely, if Y2K is going to turn out to be a financial non-event, the lack of any market instabilities here will go a long way toward killing any potential downturn in its tracks.

Moving in the *Unfolding Phase*, here is the time for the Internet-based economic "doom-brooders" such as Edward Yardeni either have to fish or cut bait, meaning either we see the dynamic of **Fortressing** and **Islanding** rise up in a serious way or these theories of economic back stabbing decimating social trust and destroying business chains will need to be quickly discarded. Of course, some of this dynamic may have already unfolded during the previous phases, especially the *Mania* one, but it's really in this phase, when the supply chain failures pile up that this dynamic should rear its ugly head in a broad-scale manner if Y2K is going to unfold in a truly dramatic and destructive manner. And again, what's dramatic and destructive about islanding and fortressing is the loss of social trust and what that will do to aggregate economic behavior. If individuals see great numbers of long-standing trust relationships evaporate overnight in response to Y2K-related failures, then perceptions of the future will change drastically and for the worse. In short, we'll clearly be in a new and largely unknown rule set.

The key dynamic to watch regarding popular perceptions of an emerging rule set is what we call **Personal GDP**—namely, the depletion of financial resources set aside to weather the Y2K Event. Everyone—every person, firm, government, etc.—will enter into the Y2K experience with certain expectations regarding how much this is going to cost them. When this threshold is reached, meaning the money (and/or other assets) set aside is gone, perceptions of economic loss can escalate dramatically and result in a significant skewing of individual and collective decision making. Of course, the more individuals and organizations plan for a "tall" Bell Curve, but instead find themselves riding the stretched-out "far side" of a curve that never seems to end, the worse this dynamic becomes.

The *Peak Phase* in the Business timeline is defined as a *de facto* **Cash Economy**, meaning a virtual de-creditization of the economy as social trust evaporates and almost nothing gets done unless cash or other hard "currencies" (depending on what society you're talking about) are involved. Realistically speaking, within the hardest hit pockets of a country, we'd see cash economies sprouting up, without the country as a whole devolving to a cash-on-demand status (meaning the semblance of normality tends to be preserved in official circles). The obvious model for this type of situation would be Russia since the fall of the Soviet Union. Having said that, we'd note the Russian tendency to muddle through—with great day-to-day effectiveness—what advanced Western countries would consider a state of almost complete economic collapse; in other words, *our worst nightmares are often many countries' normal operating procedure*.

To go from the *Peak* to *Exit Point*, countries may well have to face the task of some sort of **SME Triage**, meaning some sort of economic or political response to substantial numbers of Y2K-related business failures among Small and Medium Enterprises. We don't have any simple answers on this one; we just note the potential rapid loss of jobs connected with SMEs and the tendency of many governments around the world to consider that a serious threat to political stability. For SME failures to occur in great numbers, one would imagine the confluence of three dynamics over a substantial length of time:

- Direct Y2K failures leading to failed business operations
- Islanding and fortressing of extant business partners by firms in response to failed business operations
- Increased exposure to litigation liability for breached contracts or product liability issues.

We define the *Exit Point* as **Winners Crowned**, meaning the identification of individuals or firms that are perceived as having flourished during the Y2K-induced economic crisis and who, by doing so, set the tone for whatever **New Rules** characterize the resulting economic legacy of Y2K. This, of course, will be greatly determined in most countries by the accompanying political legacy to be discussed below in the Governance timeline. A good way to think of this dynamic is to reflect on how Wall Street periodically crowns some new set of financial "giants" every X years as defining what seems to be a new model of market activity (e.g., the "quants" or "professors" after 1987). Of course, if Y2K is substantial for a country, we could see the "winners" emerging with a far greater concentration of wealth, particularly if many SMEs are to die off or be absorbed by larger firms. If this occurred, one could easily consider—yet again—that Y2K fits well within the paradigm of the New Economy, which is described by many as featuring a high SME failure rate and a winner-takes-all playing field.

## The Social Response Timeline in Detail

Moving from left to right along the timeline:

In the *Mania Phase* we cite the ***Truth is Out There*** dynamic signifying large amounts of popular distrust of the Public Transcript put forth by government and business leaders regarding Y2K potential impact. By some estimates, for example, there are more than 100,000 web sites currently devoted to "surviving Y2K." Clearly there's a significant market for this sort of material, meaning that the "good cop, bad cop" approach pursued by many authorities (i.e., Don't worry! But get ready!) tends to drive a percentage of the populace to non-traditional sources of crisis-related information. In short, many people "out there" assume that the "full story" is somehow being "kept from them," while the "official story" is not to be fully trusted. It's not hard to see why there's so much mistrust. It is very hard to determine who is an "expert" on Y2K, much less what good data is, and very little of the material you see on the subject expresses anything close to ambivalence. In the end, the fine line between proper preparation and overreaction is almost impossible to pin down. Meanwhile, advocates on both sides of the argument constantly deride the other's attempts as "misinformation" of some sort or another.

Not surprisingly, the dynamic to watch as we move from *Mania* to *Countdown* are ***Rumor Mills***, for when people don't feel that authorities are being fully transparent in terms of information sharing, then they tend to seek out and respond to whatever informal information they can get their hands on. The Internet naturally plays a huge role in this, as does the mass media, but it is really the face-to-face communication that tends to hold the greatest sway over popular actions as uncertainty rises. That's only natural, since people tend to turn to others close to them for advice and collaborative thinking during crisis periods. So, as a general rule, the greater the popular perception of looming crisis, the greater the role played by rumor mills in particular, and informal communication channels in general, with the most dangerous situation being when authorities have effectively lost the attention of the public regarding preparations for crisis management. It is also fair to say that rumor mills tend to work more effectively in less developed economies than in more advanced ones, where access to mass media is virtually universal. Finally, it's probably accurate to say that rumor mills will generate increasingly wilder stories (e.g., urban legends) as the 010100 threshold looms, therefore many of the activities of authorities near the end of the Y2K build-up will be focused on stamping out "bad information" vice spreading "good information."

When the *Countdown Phase* ensues, ***Information Overload*** seems inevitable for all societies not undergoing some greater sort of "crisis," whatever that could be. Mass media coverage of the Millennial Date Change Event and "looming Y2K crisis" is likely to reach epidemic and epic proportions, in large part because the latter presents almost everything one could ask for in terms of a global media event: great uncertainty, great danger, great debate, lots of conflicting expertise eager to sway public opinion, a worldwide "playing field," and a worldwide audience. Toss in the world's largest party and we're

talking some high ratings, especially for news programs which increasingly specialize in releasing frightening bits of information to the public over a stretch of time as a way to ensure continued loyalty. Since bad news sells better than good, it goes without saying that much "bad news" will be "found" by the mass media during the last few weeks of 1999. The effect of all this "bad news" can have one of two effects on the public: scare them into action or numb them into inaction or indifference. Much will likely be determined by individual exposure to network failures prior to 010100 that can be causally linked to Y2K: if no to little exposure happens, the heavy media coverage is likely to incite indifference, whereas significant exposure may incite some level of panic among those "convinced" by their experiences.

Moving from *Countdown* to *Onset*, we watch for the dynamic we entitle, *Final Solutions*, by which we mean individual citizens and organization actively engaging in "end-game" strategies decided upon weeks or perhaps even months earlier. This aggregate pursuit of what could be highly idiosyncratic coping (or simply celebratory) strategies may well be disorienting for society as a whole, for it may appear to all that significant segments of the population are clearly "going their own way" at the last moment, thus decreasing social trust as a whole as the 010100 threshold looms. Since, in many cases, the exhibited behavior may be the first public expression of that which up to now has been a strictly Private Transcript, the sudden shift in behavior by many may ratchet up the level of uncertainty and fear for the society as a whole. Of course, the classic story here is the one concerning survivalists or apocalyptics "heading for the hills" at the last moment, determined to "escape the chaos." Another variant that may wreak serious social harm is that small minority of mentally unbalanced individuals who may seek to "go out with a bang" on their own terms, raising the potential for a cluster of Jamestown-like mass suicides, Littleton-like shooting tragedies, and/or Waco-like stand-off between authorities and heavily-armed religious cults. In this regard, we'd argue that special security attention be given to religious shrines or meccas, or any place with strong significance for typically marginal social elements with a history of acting out violently during times of stress.

When the *Onset* finally hits, there will simply be a *Will to Party* that is both inescapable and profoundly powerful. To a great extent, the public desire for mass celebration should be accommodated to the greatest degree possible while seeking to reduce network pressures and limit unmanageable concentrations of people. Typical celebrations magnets, such as religious meccas, capital cities, and cultural landmarks, are likely to be packed to the breaking point, and while that presents significant security problems, attempts by authorities to block access are likely to be counterproductive. Naturally, the "world's largest party" is likely to produce a corresponding large amount of personal injuries, sporadic low-level violence, spontaneous riots, alcohol- and drug-related crimes and medical situations, and so on and so on. Almost none of this will have anything to do with Y2K in and of itself, but instead will simply reflect the nature of the Millennial Date Change Event in the country in question. If Y2K failures do disrupt such celebrations, there should be cause for alarm and yet, most people "trapped" in such situations respond quite nicely by rising to the occasion according to the spirit of the celebration. This is not to say that riots, violence, etc., won't happen, but that the additional burden of Y2K-related failures is unlikely to exacerbate their normal course to any significant degree. In

short, it will be a wild party no matter what, and if Y2K "joins in," its immediate effect is likely to be negligible.

As we move from the *Onset* to *Unfolding*, an inevitable dynamic will be one of ***Panic Release***, meaning social expressions of exasperation, anger, fear and loathing. The possible angles are many, with the following being just a few:

- Some will be exhausted by all the recent uncertainty, build-up, and celebration
- Others will be angry that Y2K turned out to be a "sham"
- Still others will be angry that Y2K turned out to be "far worse" than authorities "let on"
- Some will be angry at the lack of the "apocalypse," "rapture," or supernatural intervention in human affairs
- Others will be convinced that such "end times" are indeed unfolding
- Still others will be frightened by all the "odd behavior" they seem to be witnessing.

In short, the Millennial Date Change Event, along with the threat of the Y2K Event, is likely to elicit a strong build-up of social tension, not all of which will be spent in the celebrations surrounding 010100. There will be burnout, a sense of letdown, along with heightened anxiety that Y2K "has finally begun." Many, if not most of the population will take all this in stride, but a significant minority will not. The big question will be whether that minority's actions will trigger broader social responses that authorities cannot control or simply be contained by authorities and written off by the larger public as the "typical nonsense of the extremists/troublemakers/wackos."

Assuming a significant *Unfolding* of the Y2K Event, the next dynamic of note is the ***Iatrogenic Zone***, or what we like to call, "average people doing stupid things under duress"—something we're all familiar with. This is not so much panic, as the purposeful attempt to "fix things" that only leads to making them worse. Tackling real and identifiable problems is only a small portion of this dynamic (e.g., "experts" who attempt to "fix" things, armed only with their blinding ignorance), because the real damage tends to be done by those individuals or groups that target the imaginary, insignificant or unrelated "Y2K problems" with great gusto and, by doing so, create follow-on failures and clouds of confusion about actual Y2K causality. This dynamic is a key one for extending the Y2K Event beyond its minimal boundaries and into the realm of an unanticipated disaster, with the paradigm being the stunned local official staring into the news reporter's camera stammering, "We had no idea that people were going to . . ."

As we watch for a transition point from *Unfolding* to *Peak*, the crucial social dynamic is what we call the ***Trigger Effect*** (referencing the 1996 Amblin Entertainment movie of the same name noted earlier in this report). As stated before, most people do not panic

during disasters, but rather rise to the occasion nicely, with only a very small minority succumbing—temporarily—to so-called disaster shock (i.e., a massive mental reordering of priorities following a cataclysmic event). The Trigger Effect doesn't refer to either of those two realities, but rather to one that appears much further down the road in a crisis—namely, when "battle fatigue" sets in. A particularly acute trigger of this sort of "crossing-the-line" behavior is the perception that either the crisis is being artificially drawn out by uncaring authorities ("Why don't they fix things faster?") or that recovery rates are unequal "for a reason"—meaning preferential treatment is being afforded by authorities. Nothing brings on the "short fuses" faster than the sense that "we're no longer in this together," whether the "they" are those receiving preferential treatment or the slow-footed authorities suspected of tending to their own needs first.

The Peak situation is obviously the most volatile phase in the social sphere, for it is here that group anger boils over and looks for ways to express itself. Typically, that means the targeting of small, easily identifiable demographic groups toward whom the majority has harbored long-standing resentments, usually over a sense of economic injustice ("They have exploited us long enough!"). **Scapegoating**, or the dynamic of targeting relatively weaker groups for persecution, is nothing more than the age-old practice of human sacrifice in light of "unexpected" and "unexplainable" disaster (meaning, in a practical sense, that those truly "guilty" are unreachable, so instead, "you hate the one you're with"—with apologies to Stephen Stills). In effect, disaster seems to rain down on you from on high, and since there's nothing you can do about the "source," you appease the anger within by striking out against those nearby that you've always resented anyway. In Indonesia, for example, during the 1997-98 Global Financial Crisis, it was the ethnic Chinese that often served as scapegoats, although sporadic reports of "ninja witches" being hunted down by villagers in remote areas made for the most compelling reportage. No matter what the idiosyncratic explanations by locals for this violent behavior, it remains nothing more than the inherent human tendency to look for someone to blame and target for persecution whenever "hard times" suddenly appear and the causality seems unclear or complex.

Of course, Scapegoating lies not only in the realm of mass behavior, but often serves as a political tool by those already in, or vying for, power. For example, an embattled regime is well served by blaming the society's ills on some small demographic group and then arranging for their state-sponsored persecution (think of Rwanda, for example). Then there's the targeting of political opponents or rivals (e.g., Malaysia following the financial crisis) designed to buttress the sagging political fortunes of a leader perceived to have done poorly by his or her people. In short, "hard times" breed harsh attitudes, and harsh attitudes make for absolute solutions, which in turn make for excellent political tools for those leaders with the will and way to divide and conquer (or typically, reconquer) their own populations during conditions of internal crisis. Think of Lenin in Russia during World War I, or Hitler in Weimar Germany, and you get the picture of the potential for political tumult under the right conditions.

Can Y2K create such dire circumstances in any country? Assuming the right set of truly disastrous proportions, anything is possible. In short, our planet's recent good fortune in seeing unrest lead to greater political freedom shouldn't blind us to the potential for

equally negative outcomes. One true bright spot, though, is our hypothesis that Y2K will probably present greater political unrest potential for authoritarian states than for democracies. Why? Again, distributiveness equals robustness with regard to network failures, and democracies are simply more distributed than authoritarian regimes.

The dynamic to which authorities may have to resort to move their societies out of the *Peak Phase* and into the *Exit Point* is proving to their public that the ***Guilty Will Pay***. Now, this probably sounds a bit hypocritical following the previous paragraphs on scapegoating, but the reality is that a key motivation for scapegoating is the perception that the truly guilty are out of reach and therefore untouchable, so instead you reach for what's at hand. When authorities act to demonstrate to the public that rules still matter and those who break them will not get away with it due to the perception of unusual circumstances ("All bets are off!"), they send a strong signal that while a new rule set may be emerging, the old one still operates in familiar ways, forcing accountability in the end. Accountability is what keeps vigilantism and scapegoating at bay, for it says that—ultimately—those who break the rules will pay for their crimes. Hopefully, authorities can convince the public that state-directed retribution will remain within legal parameters, but it's entirely possible that in certain extraordinary situations, extraordinary (meaning, extra-legal) measures will have to be taken. That can sound fairly sinister from an American perspective, because we have relatively high legal standards, but in many countries around the world, definitions of extra-legal means are highly dependent on the circumstances or the crisis and cultural (in)sensitivity to losses of political liberty.

The *Exit Point* for the Social Response timeline is easily defined—namely, the broad perception that the ***"Worst is Over!"*** Once the perception takes hold that the Y2K Event has crested and we're on a downward glide path back toward "life as we knew it," the crisis effectively ends in terms of social response. Naturally, attempts by authorities to will this view into popular acceptance will probably be met with significant resistance if the gap between rhetoric and reality is too much for the populace to bear. In the best possible path, a freely operating mass media senses this spontaneous mood shift among the citizenry and "declares" victory on their behalf.

The legacy issue for the Social Response realm is the potential for ***New Faiths*** to emerge from Y2K's ashes. These faiths can be either secular (i.e., political movements) or religious based, with the key attribute being their self-perceived "birth" under conditions of great crisis. Along these lines, we cite the emergence of the revolutionary Marxist group Tupac Amaru in Peru following a tremendous natural disaster (earthquake). In short, disaster can bring people together in all sorts of ways, with political or social activism—be it peaceful or violent—a frequent long-term outcome. Given the tumultuous global changes of the 1990s, it's only natural to assume that new faiths will rise up in challenge to, or support of, new definitions of the status quo. If Y2K triggers enough social tumult, it may crystallize a larger moment in history in the minds of those either happy or unhappy with the recent transformations wrought by the end of the Cold War, the Information Revolution, and the emergence of Globalization and the New Economy.



## The Governance (AKA, Political) Timeline in Detail

Moving from left to right along the timeline:

In the *Mania Phase* we focus on the dynamic of the **Credibility Gap**, referring to the tendency of populations to distrust "official truths" put forth by government agencies on the subject of Y2K. This gap extends in both directions, meaning it includes both those who believe the state is too lax in tackling the issue and doesn't warn the public enough about its potential effects and those who believe the state is unnecessarily hyping the issue and scaring the public. The later any government began its efforts to raise public awareness and push remediation efforts, the greater the gap will be, for the public tends to respond in one of two ways:

- People assume the government "blew it" by not tackling the subject earlier, and hence is covering up its "mistakes" now
- People assume the government is "caving in" to Y2K "fear mongers" and doesn't really have a good grasp of the actual situation or resulting vulnerability.

Outside of the U.S., the dynamic carries the additional burden of potential anti-Americanism, anti-Westernism, anti-capitalism, and/or anti-technologism, for the Y2K "problem" is easily identified as stemming from any or all of those quarters and thus remains suspect in terms of actual causality ("Is it a real problem or an American scam?"). Additionally, tied to both these variants is the sub theme that either the government or the U.S. Government in particular really knows how to "make Y2K go away" but isn't "coming clean with us" for some selfish reason (e.g., profit motive, "plot" to derail the Euro's introduction).

Given this substantial level of distrust of government leadership on the issue, a crucial dynamic as we move from *Mania* to *Countdown* is any public or private sector efforts to educate the public about how to prepare for the Y2K Event, AKA **Y2K & U**-type promotional and educational material or campaigns. Obviously, the earlier and more aggressive the campaign, the better. Likewise, the more transparent and honest the campaign, the better. Sounding too ominous only scares the public either into hyperaction or inaction, while sounding too optimistic only makes people think you're holding back the "bad news." Emphasis should be on the universality of the effect and the universality of the response—"we are all in this together." Since IT-awareness is relatively scarce in many countries around the world, while work-arounds for network failures are a fact of daily life, these campaigns in many parts of the world can focus more on explaining causality than the provision of "survival information." In other words, in most places people know what to do already in response to Y2K-induced failures (i.e., the same old, same old), so authorities should focus their educational campaign on dampening any potential social backlash that could be fueled by disparities in suffering or recovery times, as well as ig-

norance of causality leading to the propagation of conflict-triggering "explanations" ("Let me tell you why this really is happening to us and why you shouldn't take it anymore!").

Once the *Countdown Phase* begins, our dynamic comes more in the form of advice, as in, "Go with the ***Authority on Tap***." By this we mean that governments should not seek to introduce special leaders, authoritative bodies, or new rule sets in the waning days of 1999, but rather should stick with the architecture of authority they (hopefully) have already put in place during the previous months. If new authorities and rules are introduced at this late date, governments are likely to trigger more distrust than trust, and more rule breaking than rule-abiding than if they simply went with what they already have—no matter how deficient. Why? Any last-minute introduction of new authority only fuels popular suspicions or fears that the government is ill-prepared and/or now is finally "coming clean" on its "secret plans" to use Y2K as a pretext for some sort of reordering of political relations either within the government or between the government and the population. *The positioning or use of military and/or security forces becomes a highly volatile issue during this phase*, for it represents the worst fears of some regarding the government's "true motives" vis-a-vis Y2K.

Such popular suspicions only highlight the government's need to get its security "house in order" substantially prior to the 010100-threshold. This is especially true in relation to the key dynamic we cite for the transition period from *Countdown* to *Onset*—the danger of the ***First Strike***. First Strike refers to the high probability that significant numbers of activist groups will seek to mark the Millennial Date Change Event by engaging in some high-profile activities—both malevolent and benign, but focused foremost on garnering mass media attention—in support of whatever cause they espouse. Most political causes or movements—not just the extreme, apocalyptic ones—tend to be very date sensitive, meaning history and the milestones of time's passage play a great role in motivating action and determining its timing. The 2000 threshold will simply be too great a target for most such groups to pass up, regardless of their motives (i.e., anything from simple self-celebration to catastrophic violence). Moreover, the rise of the Information Revolution provides new avenues for such strategies, most notably the Internet and the World Wide Web, which are likely to see explosions of released viruses and various expressions of hacktivism (i.e., politically-oriented hacking). In short, authorities should expect all sorts of groups standing up at this point and declaring, in so many words, that either "We rule!" or "We're not going to take it anymore!"

Once the Onset hits, the government's key task is ***Keeping Up Appearances***, meaning maintaining normal routines to whatever extent possible as Y2K emerges and millennial celebrations/activities are played out so as to avoid fueling any popular fears regarding the potential for social disorder. Those elements looking for opportunities to foment greater levels of popular uncertainty or fear will likewise be watching closely for signs that things are amiss. So to this end, governments must be prepared to see through to completion whatever normal routines exist for marking the beginning of the new year, with special emphasis placed on the safety of notable figures—both public and private—who may participate or attend. For example, imagine the potential uncertainty and fear engendered by the missed or failed (for whatever reason) appearance of an important re-

ligious leader at a long-scheduled and highly attended public celebration. Following this line of reasoning, governments should avoid overloading themselves with too many events and their attendant security requirements. Better to do less and do it well than do too much and risk unintended consequences. In short, stay with what you know.

Moving out of the *Onset* and into the *Unfolding*, be aware that ***Opportunists Abound***. For the same reason why we advise authorities not to overextend themselves right at the 010100 threshold, many political opportunists such as terrorists and others looking to take advantage of a decreased security environment under conditions of "chaos" will likewise probably adopt a wait-and-see attitude regarding Y2K's unfolding. Unlike the First Strike types who are so eager to make their mark with an eye toward history, these typically more malevolent actors will look to piggy-back their destructive or criminal actions on Y2K-related failures so as to maximize their impact and/or rewards. A variety of strategies can be imagined:

- Spoofing Y2K failures to induce more network uncertainty and increase popular fears
- Striking to take advantage of security failures caused by Y2K
- Taking credit for Y2K failures they had no part in producing.

Naturally, those who normally seek to play "outside the rules" are at a distinct advantage during periods when rule sets are either suspended or unclear, so authorities must assume that such elements are actively planning to exploit Y2K's unfolding in any way possible.

The *Unfolding Phase* witnesses the dynamic of ***Backlash***, meaning the potential for some segments of the population to lash out at authority over perceived failures to address whatever Y2K-related difficulties emerge and linger. Again, we're not talking about the immediate popular reaction to any potential difficulties, but rather the tendency for negative emotions to emerge as the period of suffering drags on. Obviously, the Most Vulnerable segments mentioned above are most likely to serve as "tinder" for any such backlash, highlighting once more the great utility in assuring their basic needs during the Y2K's unfolding. Governments should focus crisis management and response efforts on Y2K causes vice symptoms, although the latter requires special efforts if more vulnerable segments of the population are affected. Public relations efforts are paramount here, especially any efforts by leaders to show that they are aware of and responding to public "pain." The key goal of the government, though, should be on gathering sufficient intelligence so as to manage public perceptions of the "time remaining" in the Y2K "crisis." Obviously, honesty is the best policy here, so transparency in all matters should be the top priority in all state-public information flows.

The dynamic to watch out for as we move from *Unfolding* to *Peak* is the appearance of the ***Answer Man***, or the political and/or military leader who promises a rapid reduction in disorder and uncertainty *if only* he (or she) is allowed to amass—albeit on a "temporary basis"—extraordinary power and institute certain strong measures that typically involve a drastic loss of civil liberties for the population as a whole. Of course, history

teaches us that this "temporary basis" often turns out to be a great number of years, usually ending with the "great leader's" death and the plunging of the political system into great turmoil. If such an individual is to appear under Y2K's peak conditions, his or her ideological appeal is likely to be based on anti-Americanism, anti-Westernism, anti-capitalism and/or anti-technologism. Thus the "cure" offered will likely involve sort level of detachment from the global economy, or a firewall strategy of sorts. In this way, the likely outcome of any state's Y2K "disaster" is likely to be one of systematic withdrawal versus striking out in anger against one's neighbors or the West in general. The regions where this outcome is most likely are those with the lowest development levels, i.e., with the least to lose in such a strategy.

The *Peak Phase* dynamic of greatest importance is the state's ***Mobilization Capacity*** in the face of an onslaught of popular demands for government services and general redress under conditions of social stress and perhaps open disorder. If all of the dynamics outlined above are occurring in the Network, Business and Social spheres, then the government is likely to be inundated with a flood of trouble calls, appeals for disaster relief, anger and resentment, etc. Only the most advanced states have historically exhibited a great capacity to effectively channel such a broad array of public demands in a short period of time under crisis conditions, and even there capabilities are occasionally found to be greatly lacking (e.g., the slow response of the Japanese government to the Kobe earthquake). Even in these advanced states, however, the potential universality of the Y2K Event presents a huge challenge, for crisis management of natural disasters, for example, is based on the principle of attacking the problem through a huge and rapid in-flow of out-of-area help. Outside the rather small circle of advanced economies with strong mobilization capacity, the vast majority of states around the world exhibit far more meager skill sets. A good indication of this is the exceedingly thin nature of local police in most developing states. Just like individual regions within advanced states, less developed countries face the additional burden of possibly being denied out-of-area help from those very same advanced states too preoccupied with their own Y2K problems. In short, many may dial their version of 9-1-1, only to receive a "busy signal."

Again, taking into consideration all the different Peak Phase dynamics presented in other timelines, it's easier to understand the notion that—in the political realm—desperate times often require dramatic acts be taken by those in power to maintain social control.

We call this dynamic, ***Killer Apps***, referring to bold political actions that serve to erase popular uncertainty and restore public faith in government control. At its most benign, a killer app can be nothing more than a Churchillian speech by a national leader that calms the public and draws people together in the "common cause" of recovery. At its most malevolent, a killer app can be nothing less than an authoritarian leader's liquidation of a troublesome opposition party through mass arrest and imprisonment or executions. It can be the calculated, top-down direction of ethnic conflict designed to unleash maximum violence or the imposition of martial law to avoid unnecessary bloodshed. In effect, it can be almost anything so long as it's bold and redraws the lines of uncertainty and disorder set in motion by the Y2K Event. But as with any attempt to "seize the bull by the horns," unintended consequences can abound. In short, it can be a very wild ride.

We define the *Exit Point* dynamic as the beginning of the ***Legal Deconstruction***, meaning anything from letting the lawyers "go at it" to the collapse of a coalition government and the resulting special election, to the passing of new laws, to the resignation of top government officials, to special government investigations as to "what went wrong," and so on. In short, the legal deconstruction is nothing more than the resumption of standard government procedures for "digesting" a crisis experience and moving back to "life as we knew it." Obviously, this is where many of Y2K's legacy issues will be dealt with. Likewise, this is where the great social debate will be held as to whether Y2K represented a unique, almost exogenous event akin to an Act of God, or the harbinger of what instability and crises will look like in the next century.

The legacy issue of the political realm is Y2K's potential to alter leadership rosters. Obviously, Y2K will occur on someone's "watch," so popular perceptions of the current government's handling of its crisis management duties will determine the likelihood of turnover by either legal (e.g., elections) or extra-legal (e.g., revolts) means. ***New Rulers*** are likely to arise on the basis of:

- Popularity untainted by the crisis (e.g., leaders in exile or out of power)
- Popularity achieved during the crisis (e.g., military or technically-focused leaders)
- Popularity on the basis of representing a stark alternative (e.g., so-called Green or anti-technology/development leaders, those advocating a "simpler lifestyle" or a "less Western lifestyle," those advocating a return to "better values")
- Willingness to take advantage of disorder through bold political means (e.g., revolutionaries, dictators).

Looking across the other legacy issues defined earlier (*New Faultlines, New Rules, New Faiths*), it's not a great stretch of the imagination to say that Y2K, if it were to unfold as a global event of significant disturbance, has the potential to represent a turning point in human history, coming as it does on the heels of the end of the Cold War, the rise of Globalization, and the unfolding of the Information Revolution. Then again, history is rarely scheduled as neatly as Y2K.

---

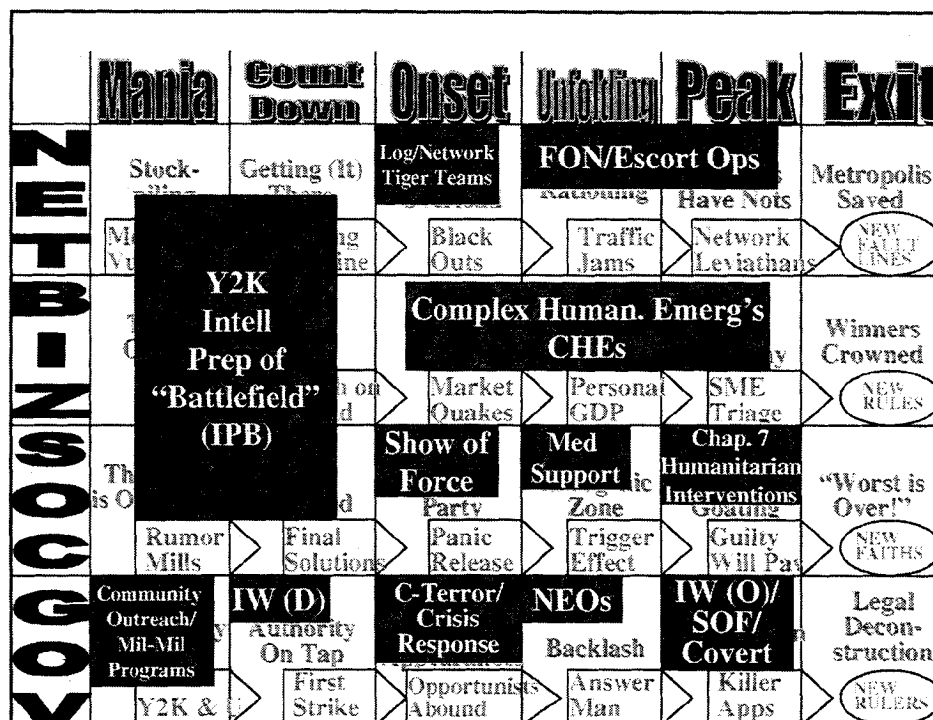
## VI. Some Preliminary Thinking on CINCs' Strategies

### Missions the U.S. Military Might Have to Perform

Slide 25 presents a list of missions we think the U.S. Military could be called upon to perform across the six-phase timeline of our Y2K Scenario Dynamics Grid. We don't mean—by any stretch of the imagination—to suggest that all of these missions are likely to be performed. Rather, we're simply hypothesizing what the U.S. Military could be called upon to do if the National Command Authority (e.g., the President) saw reason to respond to any of the particular dynamics listed below with regard to any country or region of the world. Like the Scenario Dynamics Grid itself, this is another "smorgasbord" listing of possibilities, designed to orient U.S. political-military decision makers as to the potential breadth and scope of the problem.

Along those lines, you'll note that we're not talking here about inter-state wars or full-blown military "sneak attacks." Instead, our advice is geared more to U.S. Military interventions abroad in states or regions undergoing significant dislocation and dysfunction as a result of the Y2K crisis. As such, note also that we really haven't ginned up any new or exotic "Y2K missions." That could reflect the limits of our imagination, but we think not. Rather, our list speaks to the great breadth of missions that the U.S. Military already undertakes on a regular basis all over the world. It also reflects the underlying reality that if Y2K is going to be all about the breaking down of connections and infrastructure, then the military remains—to the extent its own Y2K house is in order—ideally suited to responding to such crises if they are deemed in the national security interests of the United States.

In short, the military (really, *all* militaries) are built around the principle of *making things move and work under conditions of great environmental distress (i.e., war) or where infrastructure is lacking (i.e., remote or austere locations)*. Of course, given the logical localizing effect of any significant Y2K unfolding (i.e., communities cut off from one another and outside help in general), local resources will be the key—thus the useful emphasis on grass-roots responses wherever possible. Just as obviously, we note that, in the grand scheme of all things global (such as Y2K), militaries in general represent a relatively scarce resource that should only be used in a strategic fashion. Simply put, militaries in general, much less the U.S. Military, cannot be the cure for whatever ails the world as a result of Y2K. This resource represents but one of many social assets that can be applied to triage what may turn out to be a very broad and interconnected problem.



Slide 25: Possible U.S. Military Missions Arrayed Across Scenario Dynamics Grid

So, if Y2K turns out to be significant and long lasting in the manner suggested by our six-phase scenario time line and associated dynamics, we foresee ten mission categories possibly arising:

- *Y2K Intelligence Preparation of the "Battlefield"* (Network/Business/Social Response-Mania/Countdown) refers to the normal pre-crisis/conflict gathering of information relevant to possible downstream missions. As such, any CINC is likely going to want to know the answers to four essential questions:
  - Which countries in my AOR (Area of Responsibility) are most vulnerable to Y2K?
  - How may the U.S. Military intervene most effectively to help nation-states restore network operations?

- Who may seek to take advantage of Y2K to pose security threats to U.S. interests in the region?
- How much may Y2K be "worth" to the United States in this region? And what are we as a nation willing to pay for it?
- **Logistic/Network "Tiger Teams"** (*Network-Onset*) refers to sending specialized personnel into a particular country to help authorities bring crucial network nodes and/or facilities back online during the onset of the Y2K event. Since such assets are typically scarce resources, any such efforts are likely to be focused on host nations where U.S. military bases are located so as to ensure sufficient infrastructural support to allow continued operations. Beyond that we're talking about either key strategic allies or key network junctures that support the global economy—usually one and the same.
- **Freedom of Navigation/Escort Operations** (*Network-Peak/Exit*) refers to role the military can play in providing security for the transport of essential resources during periods of crisis when criminal or rebel elements tend to be more bold. As we've learned in previous interventions abroad during Complex Humanitarian Crises such as Somalia in the early 1990s, it's not enough to guard relief supplies at key nodes (usually metropolitan centers). You also have to provide security as they are transported between key nodes, for it's there where the pirates, bandits, Mafia or rebels tend to lurk, thus exacerbating the already bad resource strain.
- **Complex Humanitarian Emergencies, or CHEs** (*Business-Onset/Unfolding/Peak*) refers to a total breakdown of the civilian economy and the resulting loss of social and political control by authorities, otherwise known as a "failed state." What happens here is typically the Non-Governmental Organizations (NGOs) and Private Voluntary Organizations (PVOs) of the international relief community come to the fore and administer broad-scale relief, while the U.S. Military or United Nations Peacekeeping forces provide infrastructural assistance (e.g., logistics, essential security, basic government services) designed to help local authorities "get back on their feet" and resume political control over a reasonably stable economic and social situation.
- **Show of Force** (*Social Response-Onset*) refers to prepositioning of military assets or troops at any location within a CINC's AOR so as to signal U.S. resolve regarding, and the capacity for responding to, threats to U.S. national security, to include threats to friendly or allied governments. This is obviously a tricky thing to figure out beforehand with Y2K, because it won't necessarily be clear which situations of value to the U.S. will be threatened by Y2K, or when. Nonetheless, certain key relationships or situations are routinely identified as possessing high U.S. national security value, and these are likely to receive special attention as the 010100-threshold approaches.
- **Medical Support** (*Social Response-Unfolding*) refers to the Iatrogenic dynamic by which ordinary people do stupid things under conditions of duress and end up



hurting themselves in significant numbers, either by injury, the spreading of disease, or poor responses to physical deprivations brought about by network failures. Obviously, we're talking here about situations of sufficient scope to overwhelm local medical response capacity, which, in many nations around the world, is rather limited in comparison to the United States.

- **Chapter 7 Humanitarian Interventions** (*Social Response-Peak*) refers to the potential for Scapegoating during the worst periods of any Y2K event, and the potential for military interventions designed to protect the targeted demographic group by either providing safe havens or repelling/disarming those inflicting the violence. This can range from spontaneous riots to top-down directed efforts at ethnic cleansing. Along these lines is the potential for certain governments or political movements to target members of opposition groups opportunistically in conjunction with the Y2K event.
- **Military-Military Programs** (*Governance-Mania*) refers to the typical U.S. military cooperation with foreign militaries that we conduct on a regular basis around the world, with the notion here being that such activity should be focused on raising local military awareness of the possible Y2K scenario dynamics that may arise in any one nation or region. Likewise, if any CINC engages in training and/or exercises for the 010100-turnover, serious consideration should be given to including as many allied militaries as possible within any AOR. In short, outreach ends on 010100, so it's use or lose it.
- **Information Warfare/Defensive** (*Governance-Countdown*) refers to protecting the critical information infrastructure of the United States and its military/diplomatic facilities around the world against the First Strike potential of those elements that would mark the 010100-threshold by engaging in protests or criminal or terrorist acts. Obviously, the U.S. Military must be most concerned with maintaining its own capacity for tracking events globally, for once lost, our collective ability to manage any subsequent crises evaporates. Once secured, though, any capacity we may offer to allies and friendly regimes in terms of facilitating their own defenses against such attacks represents a significant value added to international security during this potential global crisis. Likewise, this experience may end up telling us much about what the U.S. may be able to offer allies in the future under the rubric of an "information umbrella" akin to the nuclear umbrella of the Cold War era.
- **Counter-Terrorism/Crisis Response** (*Governance-Onset*) refers to standard counter-terrorist operations and generic crisis response capabilities every CINC possesses. The key issue here is not how to apply these assets, but where, when and why? Other than the obvious threat to U.S. citizens and facilities abroad, the trick will be in determining which situation is worthy of a U.S. response, and which should be allowed to play out under strictly local conditions involving local players—a sort of "let it burn" strategy. What will be unclear during the 010100 transition is whether any outbreak of terrorism or crises represents a one-shot

deal, or the beginning of a lengthy wave that will feed off a subsequently significant unfolding of the Y2K Event. If the former holds true, then any 010100-centered outbreak would logically be dismissed as so much "white noise" associated with the Millennium Date Change Event, with U.S. assets better held in reserve for other, possibly far larger crises. If the latter were true, then an early-on blunting of such activity could prove decisive in the end.

- ***Non-Combatant Evacuation Operations, or NEOs (Governance-Unfolding)*** refers to the evacuation of U.S. citizens from foreign countries when broad-scale threats arise as to their safety. With regard to the Y2K scenario, this corresponds to the dynamic of Backlash that may unfold as Y2K's breadth and depth become more apparent and people grow angry with authorities for not preparing better, not telling them more in advance, etc. Since Y2K is easily identified in many cultures with the United States and the West in general, U.S. citizens and firms operating abroad may make inviting targets for those local elements (either public or private) seeking foreign scapegoats to "atone" for whatever economic or social dislocation results.
- ***Information Warfare/Offensive, Special Operations Forces, Covert Operations (Governance-Peak)*** refers generally to the range of extraordinary or special military operations that are logically considered as being "on the table" if U.S. national security interests are subject to grave risk abroad during the height of any Y2K-related political crises. In essence, if countries of high value or interest to the United States are experiencing a peak-range confluence of Y2K-triggered dynamics as described by our model, it's only reasonable to expect that we'd consider using such extraordinary instruments of influence.

Again, looking over this list of possible missions, one is tempted to wonder whether or not we've lent too much drama to the Y2K Event. But understanding our goal of thinking through the permutations of a significantly disabling global unfolding of Y2K, we come away from the list less impressed by what we've included than what we've left out: specifically combat operations associated with a major regional contingency. While there's nothing to say that a major regional contingency (also known as a war) can't happen during the Y2K Event, we note that even this stressing rendition of a generic Y2K scenario doesn't easily lend itself to contemplating such large-scale scenarios. To repeat, Y2K impresses us as a localizing phenomenon more likely to create civil strife and internal breakdown in political order rather than trigger inter-state conflict. To the extent this is true, U.S. Military operations in response to Y2K-related crises abroad will fall wholly under the rubric of Military Operations Other Than War (MOOTW), meaning that if Y2K represents a harbinger of global systemic crises of the 21st Century, it may represent a significant reordering of U.S. Military force structure and operational priorities.

## Primary Tasks, Strategic Choices, & Key Uncertainties

Slide 26 presents a CINC-specific version of the Scenario Dynamics Grid which focused on the primary task CINCs face in each scenario phase, plus the main strategic choice and key uncertainty each faces in making that choice. Obviously, we presume a lot here, as any CINC is going to understand his AOR a lot better than a bunch of academics sitting in Rhode Island. But, going with the proposition that it's always easier to respond to a straw man than gin up ideas from scratch, we toss this CINCs' Scenario Strategy Grid out on the table to start the conversation.

In the *Mania Phase*, we see the primary task as **Update existing plans**. Again, our list of "Y2K missions" is fairly standard, and there's almost nothing we can tell a CINC about doing any of those tasks better. What we think needs to be done, though, is a review of the extant plans—a scrubbing, if you will—to take into consideration the environment within which those standard missions may occur. So while the plans may largely remain the same, the execution may differ somewhat during the Y2K event due to the dynamics we presented earlier, not to mention the Y2K vulnerabilities faced by the military itself, especially in the area of host-nation support.

The strategic choice here is the **Degree of outreach**, meaning how much does the CINC open up to countries (both friendly and not-so-friendly) within his AOR regarding the common and individual security challenges they may face in the coming months? As with any position of high authority, this is a very tricky question that involves walking a fine line between motivating your audience and scaring them into either misdirected action or inaction. Probably the stickiest issue here involves the sharing of information or intelligence, for, as with so many aspects of the Y2K Event, this particular issue will tell us much about the price of secrecy and the promise of transparency.

Finally, the key uncertainty here is the typical \$64,000 question: how vulnerable is the AOR? Our back-of-the-envelope analysis suggests the following:

- EUCOM probably faces the least challenge of the four warfighting CINCs, since Europe as a whole probably does fairly well.
- SOUTHCOM faces some real challenge, because several countries in Latin America may do quite poorly, although the security risk here will be low and the focus on relief support.
- PACOM faces even more challenges, because many large economies in Asia may do quite poorly, and because there are key security tensions in the region (e.g., Koreas, Pakistan-India, Indonesia).
- CENTCOM probably faces the biggest challenge of the four warfighting CINCs, since the Mideast as a whole has done poorly in Y2K remediation and is quite vulnerable in terms of having centralized, monoculture economies paired with relatively authoritarian political regimes.

	<b>Mania</b>	<b>Count Down</b>	<b>Onset</b>	<b>Unfolding</b>	<b>Peak</b>	<b>Exit</b>
<b>TASK</b>	Update existing plans	Exercises & ramping up C2 focus	Intell	Con-sequence Management	Juggling resources	Gracious hand-off
<b>CHOICE</b>	Degree of outreach	Force posture	Move vs wait	Triage: what and where?	How much do you throw in?	When to declare victory?
<b>?</b>	How vulnerable is AOR?	<u>Resources</u> homeland vs CINC's	<u>Unknown Unknowns</u> still out there?	Troop morale	<u>Resources</u> CINC vs CINC	What's left over?

Slide 26: The CINCs' Scenario Strategy Grid

Clearly, the CINCs need to do everything they can to ramp up their level of awareness regarding key individual countries within their AOR in the time remaining.

In the *Countdown Phase*, we see the primary task as **Exercises and ramping up Command and Control** focus regarding Y2K. Obviously, command personnel in the AOR field need to be up to speed as the 010100-threshold approaches, and whatever efforts can be made to train the HQ command staff that will be on hand for the first few weeks of 2000 will probably pay off. In short, no command personnel should enter the Y2K Event without receiving an immersion in the range of potential situations and dynamics they could face—thus avoiding the utterance, *I had no idea it was going to be like this!*

The strategic choice here is the **Force Posture** question, meaning does the CINC want his forces spread out across the AOR in anticipation of the 010100-threshold, or does it make more sense to have the forces pulled in and ready to move out in whatever direction seems most appropriate once Y2K begins to unfold? A big factor here, obviously, is that nature of the CINC's trust in his own networks, i.e., the more vulnerable he feels, the more likely he is to keep forces closer in to HQ and vice versa. Then there's the issue of

raising expectations by forward presence, and the possibility that moving forces after 010100 could create tensions in those areas of departure (i.e., *Why are you leaving us and going over there?*). Clearly, this is a very tricky subject full of political-military nuances. Finally, there's the issue of whether any special force posture can be justified, given the overall lack of knowledge as to how Y2K will unfold. In short, any force posture is likely to be off base in some unforeseeable manner.

The key uncertainty here is the politically charged issue of the CINCs' ability to access specialized reserves and National Guard forces for duty overseas. Therefore, as resources go, it quickly becomes a **homeland vs. CINCs** dynamic. Naturally, National Authority Command decision making will favor the U.S. domestic scene over the international scene, thus the capacity of state governors to tie up such personnel through the first days of 2000 is a given. The big question here is how long will it take for the U.S. to become comfortable enough with Y2K in the domestic arena to allow CINCs' access to these personnel for employment overseas, where their specialized skills may be crucial to many of the missions listed above.

In the *Onset Phase*, we see the primary task as **Intelligence** regarding Y2K's unfolding, with the obvious question being, What's going on that we can definitely link to Y2K? So it's not only understanding the breadth of activity across the AOR (something the CINC's staff performs on a routine basis), but also the capacity to disaggregate Y2K-direct failures from fellow travelers, secondary and tertiary cascading failures, and then also the iatrogenic factor of "people doing stupid things under stressful conditions." The only useful rule of thumb we think we can offer here is as follows: treat clearly identified Y2K "disease" wherever it triggers significant security problems, otherwise concentrate on "symptoms" of distress and assume the private sector will deal with the "disease."

The strategic choice here is the **Move vs. Wait** question, meaning when does the CINC—in conjunction with NCA directives, naturally—know enough to move ahead and assume a proactive posture. At first glance, the answer may seem obvious, as in "move when you see a problem you can deal with!" But given the fact that the 010100-threshold may represent only a small fraction of Y2K's ultimate unfolding (only 10 percent, according to the Gartner Group), there's a clear disutility to responding too frantically to the "opening shots" of what may be a far larger "conflict." Certainly, the CINC must feel confident that his own house is in order before doing anything, and how long it takes to ascertain that is not easy to predict. But once beyond that threshold, the move-vs.-wait question looms very large as a national security issue—one we must essentially resolve "in the dark" until we come to a clear consensus as to how much Y2K is worth to U.S. foreign policy.

The key uncertainty here highlights the difficult of the move-vs.-wait issue, for no matter when the CINC and NCA decide to move ahead to deal with whatever Y2K-related crises arise in any AOR, no one can be sure how many **Unknown Unknowns are still out there**. In effect, once military forces leave the security of the base or garrison, they enter into the larger process of Y2K's unfolding on the international scene and thus become caught up in the larger dynamics they seek to mitigate or mollify. A force in reserve represents an asset, whereas a force incapacitated in the field represents a liability. Once committed to the open playing field of Y2K, it may be quite difficult to "turn back the

clock" and resume any pre-game position. So while some may argue, "use it or lose it" on the employment of military forces in response to Y2K, the counter-argument may be made that, "once you use it, you may lose it."

In the *Unfolding Phase*, we see the primary task as **Consequent Management** of whatever political-military crises erupt and meet the NCA's criteria for response. Again, we see the CINC conducting standard missions under non-standard conditions.

The strategic choice here is the **Triage** questions of **what and where?** Any such thinking along these lines depends heavily on how the U.S. values Y2K in the aggregate sense—namely, what is Y2K worth to the U.S.? Without a sense of the aggregate value of Y2K, prioritizing individual crises in the manner of triage becomes difficult, unless we simply fall back on the notion that our allies come first, our friends second, and our non-friends last. However, a wholesale borrowing of the national security template for implementing Y2K crisis response may well prove to be misguided for anything other than maintaining our current security relationships around the world—i.e., it may poorly capture our long-term economic security concerns surrounding Y2K's ultimate impact.

The key uncertainty here is **Troop Morale**. For example, suppose Y2K's immediate unfolding in the U.S. is minimal and we end up committing forces abroad in crisis response actions stemming from Y2K-related problems. What might be the effect on troop morale in the field if the situation subsequently deteriorated back in the United States, or, more likely, back at the overseas base?

In the *Peak Phase*, we see the primary task as **Juggling Resources** across whatever crisis response missions the CINC might be pursuing across his AOR. As described in the Scenario Dynamics Grid, we think the military's role as Network Leviathans (i.e., making things move when the usual networks are incapable) may constitute the most crucial impact it can have during the worst points of the Y2K Event. Thus, in the end, it may be TRANSCOM that turns out to be the most important CINC-dom.

The strategic choice here is the question, **How much do you throw in?** Again, this choice revolves largely around the question, How much is Y2K worth to the U.S.? While it's easy to say that Y2K is not a problem the military can "solve," there is the undeniably reality that many states around the world will feel the strong temptation to play the blame game on Y2K, with the United States as the most logical target of anger. After all, we're the clear global leader in IT, and Y2K is largely of our "creation." After all, if you buy into the notion that a country can take credit for a technological revolution, then you certainly shouldn't be surprised that many might blame that same country for a global technological snafu—especially if it ends up dropping those countries farther back in the economic "race." Y2K may be a no-win situation for the U.S., thus suggesting a low value be assigned. But it's likewise also a potentially big loss situation in terms of foreign policy aftermath.

The key uncertainty here is the potential resource competition, **CINC vs. CINC**, as Y2K reached its peak-level impact. This would not only entail the competition over scarce resources across AORs, but also the competition between resources for Y2K-related crises

versus more traditional fellow travelers that could opportunistically appear during the same time frame. For example, suppose North Korea attacks South Korea, believing its defense is hobbled by Y2K failures. Under normal circumstances, that Major Theater War, or MTW, would automatically assume top priority, just as the far smaller Kosovo bombing campaign recently achieved. Now, it may seem completely reasonable to state that such a scenario should automatically receive top priority, but if the competing broad threat is a global economic meltdown triggered by Y2K, then must that priority status automatically be given over to the Korean scenario? Or does the Korean scenario immediately fall into some sort of quasi-Cold War domino status, meaning the U.S. must show resolve here lest the world think everything's fair game now that Y2K has turned out to be substantial. Again, it all depends on how you value Y2K in terms of U.S. short-term and long-term interests.

In the *Exit Phase*, we see the primary task as the **Gracious Hand-off**, which basically assumes that the U.S. has engaged in some collection of military interventions and/or missions related to Y2K, and now seeks to disengage itself from the environment following the close of the Y2K Event. This is nothing more than implementing your exit strategy in a graceful manner, but it does bring up the issue of what would constitute the criteria for ceasing an intervention that was triggered by Y2K-related failures. For example, if we intervene in a country because the network failures triggered mass unrest, do we leave once the network function is restored, or when the mass unrest dissipates?

The strategic choice here is the question of **When to declare victory?** Clearly, this is a crucial choice for the United States Government, for while there will be strong political pressure to declare Y2K "over and done with" domestically as quickly as possible (i.e., we will be on the eve of the presidential primary season), it seems only reasonable to expect that a different calculus may need to be employed regarding overseas situations. The U.S. will likely be viewed as a "winner" in the Y2K Event, so its behavior toward so-called Losers will be closely watched by the international community.

The key uncertainty as the Y2K Event wraps up for the CINCs is the amount of damage done to rotation schedules and overall OPTEMPO. While the civilian world might feel itself justified in luxuriating in some sort of Y2K "hangover" period, the military community will simply resume its normal duties, which, as we'll discuss below, are fairly substantial at this time.

## **How Much is Y2K Worth to the U.S.?: Thinking About Maximum Load**

Table 1 represents our attempt to develop a back-of-the-envelope measure of how many crises the U.S. Military can handle at the current time. By developing a sense of how many crisis response "chits" the Defense Department could employ during the Y2K Event, and then noting how many of those are likely to be unavailable due to ongoing

CINCDom	CRISIS UNIT	CURRENTLY IN USE?
SOUTHCOM	1	Available
EUCOM	1	In Use—Balkans
"	2	In Use—Balkans
"	3	In Use—Balkans
"	4	In Use—Balkans
"	5	In Use—Northern Iraq
CENTCOM	1	In Use—Iraq
"	2	In Use—Iraq
"	3	Barely available—Focused on Iraq
"	4	Available
PACOM	1	Available
"	2	Available
"	3	Available

**Table 1: Back-of-the-Envelope Calculation of DoD's Crisis Management Load Capacity, With Estimate of Current Load**

operations, we get a sense of how much more the DoD could handle regarding Y2K above and beyond its current activity load.

Our reasoning here is fairly simplistic. We started with SOUTHCOM, the smallest of the warfighting CINCs and decided to give them one crisis response chit, which we define as something roughly analogous to Operation Just Cause, or the invasion of Panama to capture Manuel Noriega in 1989. Given that valuation for SOUTHCOM, we decided to award the remaining CINCs the following number of crisis response chits:

- EUCOM: five
- CENTCOM: four



- PACOM: three.

That gave us a total of 13 crisis response chits of the size of Just Cause.

Next we decided how many of those 13 chits were likely to be available as of 010100. Despite the continuing activity of SOUTHCOM troops in relief efforts connected with Hurricane Mitch, we felt that this CINC would have its single chit available for use come 010100.

With EUCOM, our sense is that, between the constellation of Balkan operations and its Northern Watch (No Fly Zone) duties in northern Iraq, that CINC's five chits were all likely to be unavailable come 010100, especially given the additional burdens accruing from the ground presence in Kosovo.

With CENTCOM, our sense is that their current conduct of operations involving Iraq takes two of their four chits off the table.


Finally, with PACOM, we foresee all three chits being available at the 010100-threshold, although either a China-Taiwan or a Korea scenario could easily intervene between now and then.


Add that current level of activity up, and what you see is that, of the 13 possible crisis response chits, the U.S. is likely to have only 6 available as Y2K unfolds. Speaking geographically, the U.S. is likely to have but one crisis response chit for the Western Hemisphere, roughly two for the Middle East and Africa (thinking of EUCOM and CENTCOM as a whole), and three for all of Asia and the Pacific region. *This is a very generous calculation that could easily be criticized as overly optimistic.*

What's important to remember about this calculation is as follows: *any MTW would automatically eat up the remaining six crisis response chits, meaning a substantial Iraq, Korea, or South Asia scenario—if pursued—would effectively rule out any U.S. Military response capacity for Y2K.* In short, if an MTW scenario rears its ugly head, the U.S. needs to ask itself whether or not such a standard political-military scenario represents a value significantly greater than the aggregate global damage that may be caused by Y2K. For if the U.S. chooses to pursue an MTW scenario, it will effectively write off Y2K on a global basis as far as any military crisis response is concerned. In the end, this may be a perfectly reasonable choice, but make no mistake—it is a huge choice fraught with great uncertainty as to the long-term outcome.

## U.S. Foreign Policy Legacy Scenarios: Who Feels the Pain?

Slide 27 presents a rather simple two-by-two matrix that explores the notion of Y2K's legacy for U.S. foreign policy, something that we think the CINCs need to consider as they think ahead on their AOR strategies regarding Y2K crisis management.




		Not So Bad	Bad
 Not So Bad  Bad	Not So Bad	<b>Rorschach Test?</b>	<b>Win Battle, Lose Peace?</b>
	Bad	<b>Atlas Shrugged?</b>	<b>Sys Admin or Firewall?</b>

Slide 27: Possible Y2K Legacy Scenarios—U.S. versus World

The four legacy scenarios are built off of two very basic questions:

- How bad is Y2K for the U.S.?
- How bad is Y2K for the rest of the world?

In the best outcome (*Not So Bad* for both the U.S. and World), we predict that Y2K will go down in history as one big **Rorschach Test**, meaning each country will take from the experience that which serves them best—proximately, a rationalization of their Y2K re-

sponse strategy and ultimately, a justification of their overall economic development strategy. For example, for those who prepared much, they'll claim Y2K proved the utility of their proactive approach, while those who prepared little might claim that it was all a big hoax perpetrated by the U.S. in particular or the West and its mass media in general. By and large though, countries and cultures will emerge from the experience with most of their biases about IT intact (e.g., it's great, it's evil, it's progressive, it's destructive).

In the next best outcome for the U.S. (*Not So Bad* for U.S. and *Bad* for the World), we predict that Y2K becomes further evidence in the minds of many around the planet that the U.S. is a bullying hegemon who selfishly looks out for its own interests while trampling those of others. In effect, the U.S. will **Win the Battle, But Lose the Peace**. Y2K will be viewed by many countries that fall further behind in the New Economy race as just another power play pulled off by the United States, wherein our dominance is reasserted in humiliating fashion. After all, we created the crisis, then somehow managed the solution in such a way as to benefit ourselves while damaging the economies of others. Our motivations or our efforts in trying to mitigate Y2K's global impact will matter some, but coming on the heels of the Global Financial Crisis of 1997-98, it will seem like every global game is increasingly tilted to the advantage of the U.S. and the disadvantage of emerging economies.

In the next worst outcome for the U.S. (*Bad* for the U.S. and *Not So Bad* for the World), we predict that Y2K could trigger a strong isolationist streak in the United States. By **Atlas Shrugged**, we suggest that the U.S. would, in a fit of peak, essentially "take its ball and go home," being unwilling to "play" anymore in the global economy in the same free-wheeling and no-holds-barred manner of the 1990s. In effect, the Y2K Crisis would be a crisis of confidence for the United States, especially since it would catch us so much off guard and challenge all our suppositions that our mastery of the New Economy made us invincible to severe economic downturns. Of the four legacy scenarios, this one strikes us as least likely, but because that's so, we find it completely plausible given the shock value.

In the worst outcome for all involved (*Bad* for both the U.S. and World), we predict that Y2K would have posed a horrible dilemma for the United States: either we would have tried to play **System Administrator** to the world and worked hard to mitigate Y2K's damage around the globe, probably at huge cost to ourselves, or we would have—at some point—thrown in the towel, pulled up the **Firewall** around our nation, and simply ignored the rest of the world's pain. The key question here (beside the usual one about "How much is Y2K worth to the U.S.?) is which pathway would be less traumatic? Trying to play superpower to the world and failing? Or taking a cruelly calculating stance that says, "sometimes Nature just has to take its course?" In effect, our dilemma would be between trying to put out all the fires or just letting them burn uncontrollably, for like a raging forest fire, there may be few reasonable choices in-between.

## VII. A View From Wall Street

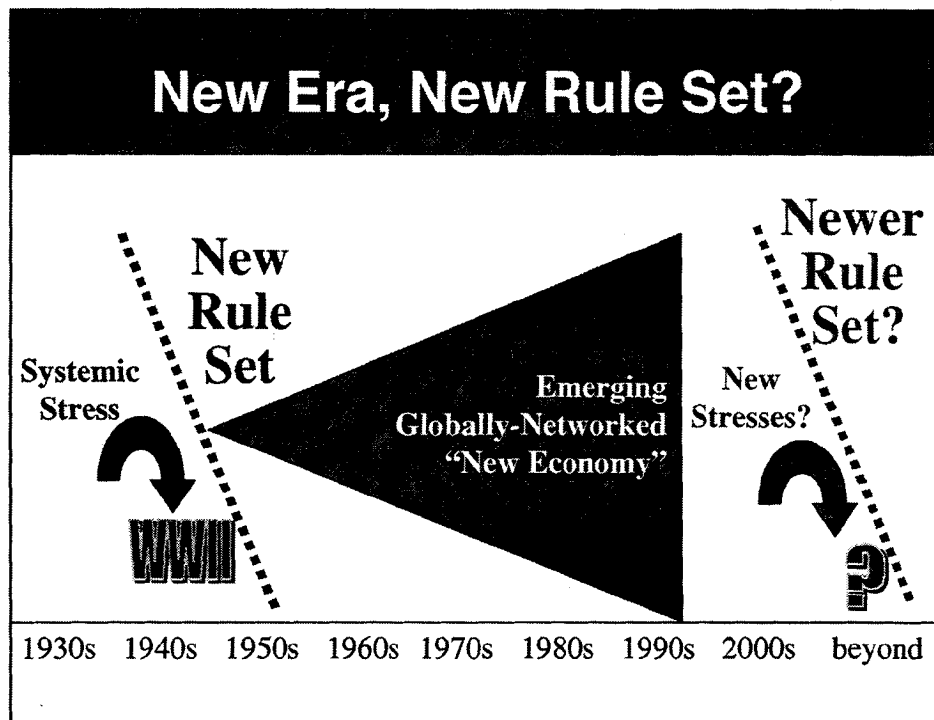
### Are We Moving to a New Global Rule Set?

If Y2K had happened back in 1995, it certainly would have been a different beast, and not just for the lack of any accompanying Millennial Mania. Back in the mid-90s we were talking about the "end of the business cycle" and the New Economy in such bold tones as to suggest that this current era of globalization (the first being from the 1870s to approximately 1929) would seamlessly and quickly knit the planet together in a win-win manner. In short, everyone was going to make lots of money and everyone was going to move up at roughly the same pace.

Of course, what's happened since then has tempered much of the naive enthusiasm about globalization, emerging economies and the New Economy. The Global Financial Crisis (Asian Flu of 1997 spreading to Russia and then Brazil in 1998) effectively left the global economy with only two vibrant engines of growth: North America and Europe. Since that time, Europe has likewise suffered an economic slowdown, leaving really only the United States and its "Goldilocks Economy" (and the U.K., to a certain extent) still riding the great 90's bull market.

When, not too long ago, the conventional wisdom on Y2K was that the most advanced, IT-intensive economies were at greatest risk, the economic worst case scenario on Y2K was that it would cripple the global economy's #1 engine of growth—the U.S. Today, with our current sense that the least advanced, and least IT-intensive economies are at greatest risk, the economic worst case Y2K scenario is that almost everyone in the global economy suffers badly except the U.S. and a few other, very similar economies (e.g., U.K., Australia, Canada, Israel). So while the former scenario predicted a near-instantaneous, TEOTWAWKI-like collapse of the U.S. economy stopping the global economy in its tracks, the latter scenario predicts a slower and broader Y2K-induced global slowdown eventually lapping up on U.S. shores and ultimately derailing the Goldilocks Economy. In essence, the shift in global recession/depression Y2K scenarios has been from "pay me now" to "pay me later," at least as far as the U.S. is concerned.

No matter which scary scenario prevails, or even if neither comes to pass, it's reasonable to say that we're currently living in a rather fragile global economy, certainly one far more fragile than we assumed back in the mid-1990s. Thus, the big picture argument for why Y2K could play a crystallizing role in terms of forging a new global consensus for international financial reform (e.g., more controls over capital flows, greater transparency among hedge funds, better accounting in emerging economies, revamping the IMF and World Bank, dollarization of certain economies) arises less from the notion that Y2K in and of itself is THE cause of a global downturn than the notion that any associated slow



**Slide 28: Time for a New Rule Set for the International Economy? (repeat of Slide 3)**

down tags Y2K as an identifiable culprit that crystallizes in many people's minds all that's wrong with the current global financial system (i.e., too given to wild periods of break-neck speculation and financial tumult). This argument was originally suggested in Slide 3, and is repeated in Slide 28.

To repeat the basic argument: the origins of the current Global Rule Set dates back to the Great Depression of the 1930s, which ended the planet's first great period of globalization from roughly 1870 to 1929. That global economic downturn constituted a drastic systemic stress that gave way to World War II. Following that experience, the great powers (at least in the West) essentially swore, "never again," and decided to erect a new international order, or rule set (e.g., Bretton-Woods, GATT, UN, IMF and World Bank), to prevent the 1930s style economic nationalism or protectionism from ever occurring again. Led by the United States, the Western great powers were eminently successful in this effort, and the lasting fruit of their collective labor was and is the globalized economy we now enjoy. This feat, far more than the story of the Cold War, represents the greatest historical legacy of the post-WWII period.

The question that arises in the late 1990s, however, is whether this new, globalized, IT-driven economy has advanced to the point of outgrowing the "new rule set" of the late 1940s and early 1950s, in effect creating the need for a new rule set for the New Economy. Those who make this call basically point to the systemic instabilities since 1997 (or even back to Mexico's peso crisis of 1994) as evidence that the old post-WWII rule set is now antiquated, thus endangering this second great period of globalization to the same fate as the first. So it's into this somewhat shaky rule-set environment that Y2K appears as 1999 draws to a close, the basic question being, With the global economy so fragile right now, how big of a disruption would Y2K need to be to throw a wrench into the world's financial machinery, finally crystallizing a broad-scale effort to rewrite its operator's manual?

## **Will There Be A "Flight to Quality" Prior to 010100?**

In our May workshop in New York City, hosted by the brokerage firm Cantor Fitzgerald, we presented out six-phase Y2K Event timeline to a group of Wall Street investment experts, traders, bankers, brokers and research/media types, exploring the complex question, How would global financial markets adjust to, and process the unfolding of, such a broad, stressing scenario?

Slide 29 presents "what we heard" from Wall Street in terms of the *Mania* and *Count-down* phases, or basically the build-up toward the 010100-threshold. In this phase pairing, we proposed that Flight to Quality was the most likely global financial dynamic in response to the looming Y2K Event. While simplifying some of the arguments greatly, we arrayed the major points offered by participants into two distinct camps—here, pro-panic and anti-panic.

We'll start with the pro-panic arguments, the first of which is the standard grip about the great bull market of the 1990s—namely, all this success makes everyone feel like they're geniuses and thus the market's never had so many idiots spending their money so foolishly as right now. While that's been the standard cry of many "bears" for several years now, it certainly carries a lot more weight after the near-global meltdown of 1997-98, when the global market run-up in emerging markets reached great "bubble" proportions and finally collapsed in on itself. Naturally, when the most disastrous bet made was spearheaded by a highly respected U.S. hedge fund fronted by two Nobel Economics Prizewinners (Long Term Capital Management), the notion that the average investor may be in well over his or her head becomes a lot more believable.

Another pro-panic argument says that the U.S. financial markets are long overdue for a correction, noting that much of the recent run-up in stocks has been concentrated within a very small pool of highly successful New Economy firms such as Microsoft, the Silicon Valley giants (e.g., Oracle), the Internet constructor firms (Cisco), and all those "anything.com" IPOs. Naturally, if so much of our optimism about our collective economic

## Mania & Countdown: What We Heard

### Pro-Panic

- Market's never had so many uninformed investors
- Long overdue correction
- Worry over US domestic Electronic Herd (AM radio crowd)
- Congress on sidelines over liability . . . ?

### Anti-Panic

- '97-98 global crisis was vaccination against F2Q
- F2Q will be into US securities and MIDCAPs; just evens things out
- Fed's ready to make \$ cheap and plentiful
- Europe feels Y2 OK

Slide 29: What We Heard—Mania & Countdown (Key Issue = "Flight to Quality")

future is tied up in IT firms, then certainly a IT-triggered global economic shock would strike deep into the heart of investor confidence concerning the so-called Nifty Fifty.

Looking more to the U.S. investor, concern was expressed that all this "doom and gloom" flying over the media airwaves (e.g. AM radio) might trigger many to withdrawal their funds from the stock market as the year wound down, and as goes the U.S. flagship markets, so too could go the rest of the world's. In short, given the slim foundations of this very long-in-the-tooth bull market in the United States, it wouldn't take much in terms of investor jitters to trigger a significant stampede out of equities.

Finally, there was a nagging sense that the U.S. Congress would never muster enough will to pass a liability-limit bill that would survive a presidential veto, a bit of pessimism that already seems unwarranted, as it now seems inevitable that such a bill will be signed by President Clinton. Still, much criticism has been voiced concerning the compromise, with many strong-voiced opponents labeling the law a sell-out to big IT corporations at the expense of small and medium enterprises.

Among the anti panic arguments, the most compelling comprehensive argument was that the 1997-98 global financial crisis served to vaccinate markets against the flight to quality threat. The argument here was many sided:

- There's a lot less "gypsy" or "hot" capital streaking around the world now
- Hedge funds have come under a lot more scrutiny after the Long Term Capital Management debacle
- Emerging markets have cleaned up their act a lot by adopting far more transparency in terms of market operations, banking, and general financial accounting practices
- Global investors are now much less naive about emerging markets
- International Financial Institutions like the IMF and the World Bank have learned much from the process, and, along with the U.S. Treasury, now act more preemptively to stave off currency crises, such as the recent rescue package for Brazil
- Markets and market players have, in general, learned much about the pitfalls of the globalizing New Economy, therefore acquiring many of the skills needed to weather whatever financial tumult Y2K might toss in their direction.

In sum, this argument states that the 1997-98 Global Financial Crisis was sort of a dry run or dress rehearsal for Y2K.

A second anti-panic argument states that even if a flight to quality occurs, it will simply "even things out" financially by moving more money into securitized debt markets in general and, within equity markets, away from the so-called New Economy heavyweights into small and middle capital firms and those old market standard bearers, the cyclicals (i.e., more industrial-era firms specializing in production). While this shift might burst the Internet bubble, that's hardly the end of the world as we know it, and really only proves that no great laws of economics have been repealed by the Information Revolution. In short, much ado about nothing.

A third anti-panic argument points to the clear readiness of the U.S. Federal Reserve to keep money plentiful and cheap as 1999 draws to a close. The unprecedented step last December by Chairman Alan Greenspan to print out an extra \$50 billion for injection into the U.S. currency supply signaled that in spades. In short, this will be exactly the sort of experience the Fed was designed to mitigate, and with the impressive Greenspan at the helm, all is likely to be well in the world's financial center of gravity.

Finally, Europe feels Y2K okay as a result of going through their own vaccination-like experience: preparing for and introducing the European Monetary Unit, or Euro. Now, the oft repeated counter to this notion is that Europe's preoccupation with the Euro's introduction in January 1999 served as a huge distraction that diminished its Y2K remedia-



tion effort, thus exposing it to more danger come 010100, but many in Europe feel—much like Wall Street does about the 1997-98 Global Financial Crisis—that much good came out of the Euro experience in terms of preparing them for new levels of coordination among state governments and financial markets. Again, many Europeans feel the Euro's introduction taught them much of the New Economy skill set needed to deal with a systemic challenge such as Y2K.

To sum up this section, we note that the majority opinion here lay with the anti-panic arguments. In effect, whatever financial knee jerks Y2K could trigger were seen as falling within the normal, sometimes roller coaster-like parameters of major markets in our IT-driven, globalized New Economy—definitely not for the weak hearted, but not out of the ordinary for today's financial environment.

## Could Markets Go Broke in Post-010100 Meltdowns?

Slide 30 moves us on to the *Onset* and *Unfolding* phases, or basically the first several weeks past the 010100-threshold. In this phase pairing, we proposed that Markets Going Broke was the most likely global financial dynamic in response to the Y2K Event initial unfolding. Again simplifying the arguments, this is what we heard in terms of pro- and anti-crash rationales.

The biggest pro-crash argument concerned oil, and the argument was an unusual one. Most participants were sanguine about the oil companies themselves and the shipping of oil over the seas, whereas the biggest concern revolved around the transshipment ports and specifically, the record keeping or "admin." The reality is that it doesn't take much of decrease in the flow of oil, for example, into the United States to trigger short-term price rises. A slowdown in the range of only 5 percent is sufficient to send gasoline prices significantly upward, according to Department of Energy representatives, and once that happens, the economy adjusts accordingly to account for higher cost in such a crucial commodity. In short, that price rise alone is enough to make Wall Street sit up and take notice of the possibility of a Y2K-induced downturn.

Another pro-crash argument centered around the enterprise software systems that allow for the just-in-time supply chain margins that have come to define the New Economy. We can sum up the Wall Street thinking here rather easily: This will be a big test of enterprise software systems. If they work, they will have proven themselves in a very profound way, but if they don't, the economy could be in for a nasty surprise. Along with manufacturing, this argument points in the direction of the Flood Onset Model, i.e., the slow but inexorable "gumming up" of the supply chain "works," especially among critical component suppliers.

Another pro-crash argument concerned countries with xenophobic tendencies. In short, those states that have a hard time letting outsiders help may be in for the harder times. Taking into account that Y2K is ultimately a localizing affair to the extent it's significant,

## Onset & Unfolding: What We Heard

### Pro-Crash

- Oil probably the biggest volatility factor
- Enterprise software creates razor-thin JIT margins; do they work to manage disruptions or cause them?
- Countries that won't let outsiders help are at greatest danger
- '97-98 "flunkies" will lose out on international aid

### Anti-Crash

- Market predictions for 1Q will factor in losses
- Firm IT "lock-down" in late 99 triggers pent-up of product releases
- Usual "Jan effect" in markets + all that CASH!
- '97-98 "graduates" will be protected by int'l aid

Slide 30: What We Heard—Onset & Unfolding (Key Issue = "Market Liquidity")

most participants assume the U.S. and Europe will do reasonably well, leading to the possibility of providing immediate help to lesser-developed countries suffering worse. Thus, to the extent that such countries are politically open to this aid (i.e., "Western help for a Western problem"), they may weather the "storm" like any other complex emergency. However, if cultural norms or political values such as the desire for autarky ("We solve our own problems without the West's help!") predominate, the interconnected nature of the Y2K Event may force the West, along with neighboring states, to effectively "quarantine" the state in question, thus exacerbating the ongoing situation in a multiplicity of ways.

Finally, there was the sense that International Financial Institutions like the World Bank and IMF would be forced, for lack of funding, to turn a deaf ear to those states suffering Y2K-induced economic crashes that had not "cleaned up their acts" following the 1997-98 Global Financial Crisis. In short, if you "firewalled" your economy off from the world a bit in response to IMF calls for reform, don't expect to find yourself at the top of the list for it's attention come 010100.

Moving on to the anti-crash arguments, the first and most obvious one offered was that the markets would naturally take Y2K into account when forecasting 1st Quarter earnings estimates, with consideration given to firms that experience unusually high volume in the last two quarters of 1999 and suffer a dearth of sales in the first due to a combination of Y2K disruptions and the inevitable draw down of stockpiled supplies. In other words, so long as there's enough realistic thinking on Wall Street concerning vulnerable firms, there'll be no surprises, and since the market basically responds to "current events six months into the future," 1st Quarter activity will reflect the view of the inevitable recovery in the 2nd or 3rd Quarters, and not the immediate difficulty of the first. In sum, losses aren't the problem, surprises about earnings are the problem. But no surprises should happen if Wall Street firms and other markets do their homework. Of course, this gets us back to the problem of all that self reporting that goes into generating those Gartner Group (and others) reports, but "putting on a good face for the investors" isn't exactly a Y2K-specific problem, now is it?

A second anti-crash argument cites a perceived but not yet proven IT "lockdown" by major firms, meaning a freeze on IT purchases through the last two quarters of 1999 until Y2K passes. On this point, participants noted that IT firms had taken this dynamic into account already, and we're planning to unleash a torrent of new products during 2000. In effect, Silicon Valley saw this lull coming and is prepared to jump start the market ASAP once the Y2K Event recedes into the background. If Y2K turns out to be minor, then confidence regarding Silicon Valley and the Internet stocks should soar in combination with the expanding market moment for hardware and software firms. In short, this argument is not only anti-crash, but pro-boom.

Another anti-crash argument notes the usual "January effect" whereby markets, responding to positive earnings reports from the previous year's 4th Quarter, tends to look rather optimistically toward the future year, especially if the markets end up in positive territory after the first business week (historically a good sign of positive returns for the year). A corollary to this may be a rapid influx of cash from individual Americans who, having taken substantial amounts out of equities in weeks prior to 010100, now feel reassured enough to put their money back into play.

Finally, participants predicted that the IMF, World Bank, and the U.S. Treasury would work hard to protect those emerging economies that had suffered much in 1997-98 but had "cleaned up their acts" as a result. A good example of this would be the story that Thomas Friedman repeats in his book, *The Lexus and the Olive Tree*, where he notes how far South Korea's Ministry of Finance has come since late 1997 in terms of transparency to the outside world. In December 1997, when the country's currency was under attack by international speculators, international organizations seeking to help Seoul inquired as to the state of their foreign currency reserves, only to be lied to by the Ministry of Finance, which had claimed three times as much as it actually possessed. Learning from that mistake, and the pounding it took from the "Electronic Herd" when the truth came out, the Ministry of Finance now sends out an email at the end of every business day detailing its foreign currency reserve holding down to the last penny. In short, Y2K will show the price of secrecy and the promise of transparency.

To sum up this section, we note that the majority opinion here lay with the anti-crash arguments. In effect, however Y2K unfolds over the 1st Quarter, Wall Street thinks it and other global super-markets can adjust accordingly, with the caveat being that "you're only as smart as the information you possess."

## **What's the Likely Long-Term Market Impact from Y2K?**

Slide 31 wraps us up with the *Peak* and *Exit* phases, or basically the first several weeks past the 010100-threshold. In this phase pairing, we proposed that Small and Medium Enterprises (SMEs) Failing was the most likely global financial dynamic in response to Y2K's peak experience. Again simplifying the arguments, this is what we heard in terms of pro-downturn and pro-boom rationales.

The first pro-downturn argument centered on consumer and investor confidence within the United States, and the potential for Millenarian-engendered social unrest to sap the public's optimism about the future. For example, what would be the social climate in the U.S. if November and December witnessed several Littleton-like shooting sprees, several "Heaven's Gate" mass suicides, and one or more Waco-like standoffs between federal police forces and a Millenarian group. It would not be overstating the possibilities to say that such a confluence of seemingly "crazy" tragedies would shove the country's collective psyche into levels of fear we haven't experienced since 1968.

A second argument is more general, noting that the current global economic picture features really only one solid engine of growth—the United States. As Secretary of the Treasury Robert Rubin warned repeatedly during his last weeks in office, it's simply not enough to hope that the U.S. economy can keep the global economy moving all on its own, especially given the rather slim foundations upon which recent stock market rises have occurred (i.e., the concentration on the Nifty Fifty, or New Ecoomy/Internet/" .com" firms). Moreover, it's dangerous to assume that the IMF could do much more than help out a small handful of affected nations, given its limited resources.

Another argument turns a previous one on its head: namely, worse-than-expected 1st Quarter earnings could trigger a mass exodus out of equities, given the scary long-term perspective those numbers might create among individual investors (i.e., "Wall Street had no idea how bad it was going to be!"). Linking back to the previous negative argument concerning oil, we'd note the consensus view that no commodity cost increase could throw off earning estimates more than a rapid jump in oil prices. More obviously, a peak Y2K environment would provide the average investor with more than enough signs that the future was uncertain above and beyond what was happening in the markets.

Switching to pro-boom arguments, many participants argued that most large firms—especially U.S. ones—looked at the Y2K Event more as an opportunity to expand market shares than a threat to their existence. In effect, they're defining Y2K as a sped-up market

## Peak & Exit: What We Heard

### Pro-Downturn

- Social unrest factor can sap investor faith in future
- US cannot work as sole global engine through crisis-prone 2000 & IMF easily tapped out
- Worse-than-expected 1Q earnings might trigger mass exodus; oil as key?
- We won't know LTCM-like disaster bets until they are revealed by collapses

### Pro-Boom!

- US firms treat this as market expansion, not as strategic failure issue
- Winner-takes-all "New Economy" based on high SME failure rate anyway
- Fortressing will be based on upgrading generations
- "Great housecleaning" + Y2K-created "market efficiencies" = boom

Slide 31: What We Heard—Peak & Exit (Key Issue = "SME Failures")

experience, not some one-of-kind exogenous catastrophe that affects all equally. So-called New Economy firms stand at the forefront of this aggressive thinking, believing that the organizational and marketing skill sets they've mastered to flourish in the New Economy are well-suited to coming through the Y2K Event in good enough shape to capture market shares lost by less agile competitors. In short, they don't view Y2K as something to sit out, but rather as an inevitable set of dynamics they will encounter again and again as the New Economy matures. In their minds then, there's no escaping Y2K, so why get as good as you can at dealing with this sort of market experience?

A second pro-boom argument basically discounts the economic "threat" of high SME failure rates, noting that this dynamic is increasingly part and parcel of the New Economy anyway, where a winner-takes-all mentality prevails. We could call it a sort of "T Rex" economy, where a relatively small number of behemoths regularly gobble up (acquire or bankrupt) smaller dinosaurs (firms), which in turn are constantly being replaced by new species, i.e., start-up firms promoting a singular service or product that eventually draw the attention of the giants. If, many of our participants argued, the Y2K Event forces a higher SME failure rate for some significant length of time, then all we'll see is a faster concentration of wealth and market shares in a few giant firms in each industry, but no more of a concentration than would have happened without Y2K's intervention.

Another pro-boom argument says that if fortressing occurs, much of it will be time-based rather than business partner-based, i.e., you won't ditch your long-term partner, but you may force him to engage in some wholesale IT upgrade if his current system fails the Y2K test. In effect, this has happened in many firms throughout the remediation period, as many simply found it cheaper to replace than to fix. If this dynamic must be repeated for those who fail post-010100, it'll be hard on them financially, but doable in many instances. And for those who can manage this, efficiencies will naturally accrue.

Finally, there is the general pro-boom argument that has long been offered regarding Y2K, especially in terms of the lengthy remediation effort leading up to the 010100-threshold: namely, all this preparation for Y2K constitutes a "great IT housecleaning" for almost all firms, organizations, and government entities—one that was long overdue. In many instances, firms and governments have bought into the IT Revolution with little planning or forethought, resulting in a mishmash of systems and poor overall understanding of architecture and best practices. Y2K's arrival has forced many efficiencies in this regard and, in the long run, the economy will benefit greatly from them.

To sum up this section, we note that the majority opinion once again lay with the more positive perspective, making it 3 for 3. While it's easy to brush aside such optimism as reflecting the narrow, profit-obsessed perspectives of these oft described "Masters of the Universe," there are a number of good reasons to believe their opinions are not misplaced:

- Wall Street firms place a lot of emphasis on good intelligence
- They've got tremendous financial exposure on Y2K (i.e., incentive) and tremendous financial resources to deal with it (i.e., remediation)
- They are greatly familiar with the dynamics of the New Economy, and think Y2K (as a threat) is part of that paradigm they've spent so much time and money seeking to understand
- They're not naive about the risk, just confident that the markets can process that risk
- They see the recent Global Financial Crisis as a wake-up call that a good portion in the industry took seriously, especially in the United States.

## Summing Up An Optimistic Wall Street: Market Indicators

As a way of summing up the Wall Street perspective on Y2K as we found it, we'll present the participants' sense of where the markets would go *if Y2K turns out to be significant* (meaning these are not their predictions for markets if Y2K turns out to be less than significant). We won't offer any hard numbers here, just gross

INDICATOR @ 043099	NET DIRECTION @ 123199 Vs 043099 CLOSE	NET DIRECTION @ 033100 Vs 123199 ESTIMATE	NET DIRECTION @ 063000 Vs 033100 ESTIMATE
Gold (286.40)	Higher	Higher	Lower
Oil—Brent (16.70)	Higher	Higher	Lower
Nikkei (16701.53)	Lower	Lower	Lower
Dow Jones (10789.04)	Lower	Lower	Higher
Yen/Dollar (119.40)	Higher	Higher	Lower
Dollar/Euro (1.06)	Higher	Lower	Lower
2-Year Note (5.05)	Lower	Lower	Higher
30-Year Bond (5.66)	Lower	Lower	Lower
Fed Discount Rate (4.50)	Higher	Lower	Lower

**Table 2: Market Indicators in a Stressing Y2K Scenario**

directions, although we'll note that none of the cumulative percentage swings were greater than roughly 10 percent, meaning the group as a whole did not foresee great market instability out of line with the last year or so.

Table 2 presents the directions predicted in a significant Y2K Event across nine key market indicators based on the price levels recorded at the close of business, 30 April 1999 (last market day prior to the workshop).

For purposes of clarity, we explain the results in the following method. If the global Y2K event was significant and destabilizing, then we would expect the following trends:

- Gold would rise in cost through the start of next spring and then decline
- Oil would rise in cost through the start of next spring and then decline
- The Nikkei would decline throughout all scenario phases
- The Dow Jones would decline through the start of next spring and then rise
- The Yen would weaken against the Dollar through the start of next spring and then strengthen
- The Dollar would weaken against the Euro through the end of this year and strengthen thereafter
- The return on a 2-Year Treasury Note would decrease through the start of next spring and then increase
- The return on a 30-Year Treasury bond would decrease throughout all scenario phases
- The Fed Discount Rate would increase through the end of this year and then decrease thereafter.

Again, in none of the nine cases did the group consensus predict a cumulative swing of more than ten percent, reflecting the overall positive tone of the workshop regarding the ability of markets to manage the global risk presented by Y2K.

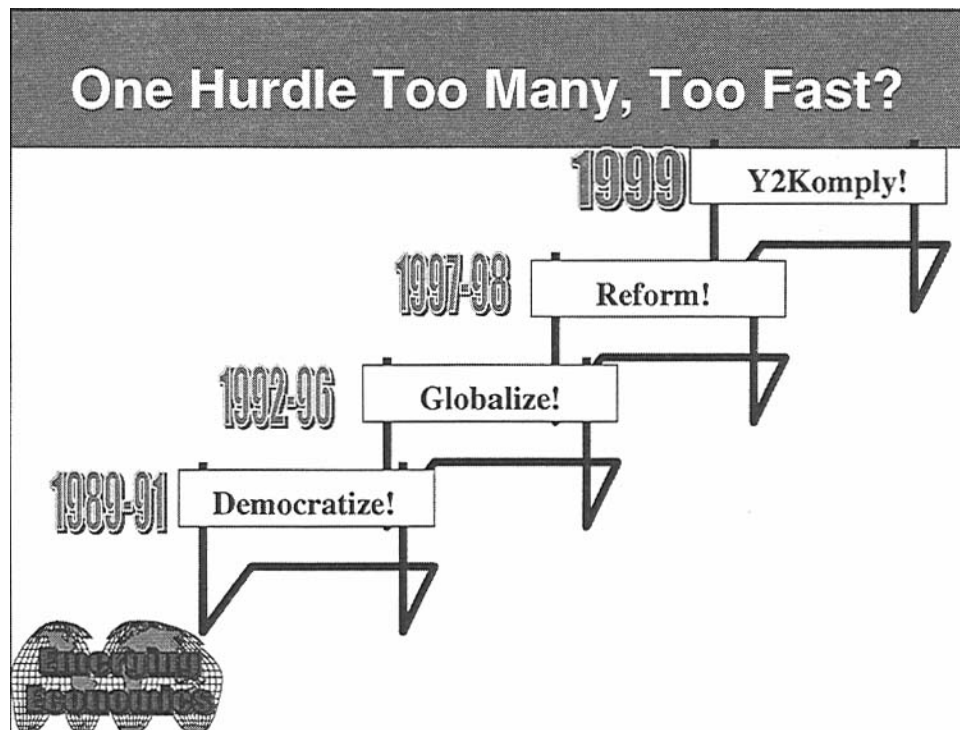
## **Spotlight: Have We Asked Too Much of Emerging Economies Lately?**

All our research to date suggests that the Emerging Economies of note (e.g., Argentina, Brazil, China, India, Indonesia, Mexico, Poland, Russia, South Africa, South Korea, and Turkey) represent a sort of "swing vote" for Y2K's ultimate global economic impact. There seems little doubt that the most advanced economies will largely do well and that the least advanced economies will largely do poorly, so the key question remains, "What happens with the Emerging Economies?"

What troubles us and some on Wall Street with regard to this Y2K "referendum" on Emerging Economies is that it comes right on the heels of a number of other challenges that we in the West has tossed in their general direction (see Slide 32).

At the beginning of the 1990s we asked most Emerging Economies to democratize their political systems—and be quick about it! The Berlin Wall had fallen and most in the West had rather unrealistic expectations in this regard, despite some heroic (and not-so-heroic) responses to this huge challenge by key states. Once President Clinton came into





Slide 32: Emerging Economies in the 1990s

power in 1992, the U.S. (largely led by then National Economic Council director Robert Rubin, who later became Secretary of the Treasury) pushed an aggressive agenda overseas to have the Emerging Economies open themselves up dramatically to U.S. financial markets. Succeeding in this effort dramatically over the next 5 to 6 years, the Clinton Administration provided rocket fuel to the course of globalization, freeing up the global movement of investment funds in unprecedented ways and, by doing so, creating some of the conditions that led to the Global Financial Crisis of 1997-98. Once the Asian Flu had started, the West, again led by the U.S., pushed hard to have many Emerging Economies "clean up their acts" and reform economic practices almost overnight. And then comes Y2K in 1999, and once again the Emerging Economies are being asked to "fix things up" and be damn quick about it!

In short, it has been one tough "row to hoe" for most Emerging Economies across the 1990s. The amount of change they been asked to endure and promote is immense. To the extent that Y2K proves to be a "separation point" between IT- or New Economy-competents and incompetents, one is tempted to ask whether or not too much has been asked of Emerging Economies as of late, and whether the West is really setting itself up for dangerous economic times ahead by adding Y2K compliancy to what already is an overstuffed and overly ambitious agenda of reform for these relatively fragile states.

## Y2K As a Sped-Up Market Period: Winners and Losers

One of the themes of the workshop was the notion that Y2K represented a sort of deadline for entry into the New Economy of the 21st Century, with the natural question for any country being, "Are you ready?"

To the extent that one can speak of winners and losers or a "global scorecard," Wall Street definitely has some opinions about who they'd expect to do well or poorly with Y2K, which we've summarized in Slide 33.

The first thing we can say about probably winners is that they'll look more like the U.S. than different. By "like" we mean they'll tend to have some or most of the following characteristics:


- Proficiency in English
- Former English colony
- Democracy; federated political structure
- Distributed economic structure; free market orientation
- Wide open social scene that's accustomed to processing a certain amount of "chaos" with aplomb
- Distributed network systems (more "parallels" than "sequentials")
- Problem-solving culture that enjoys challenges as "finest hours."

Obviously, the countries that tend to have the most difficult relationships with the U.S. tend to be the states least like the U.S., so there's where you might look for countries destined for harder Y2K experiences.

Another key attribute of probable winners is lots of transparency and rules regarding domestic and international economic behavior. The more Thomas Friedman's Electronic Herd can access in terms of good information about your national economy, the more likely it is that you'll be treated fairly (i.e., according to objective economic criteria), whereas the worse the access to good information, the more likely the Electronic Herd will interact with your economy on the basis of half-truths, rumors, and false information.

Since Y2K is considered part and parcel of the New Economy (i.e., the sort of system perturbation one just has to get used to in a globalized, IT-driven economy), the more you've mastered the skill set associated with the New Economy (e.g., ability to swap out partners at the drop of a hat, strategic alliances to hedge against uncertainty, rapid adaptation to market shifts) the better off you'll be with Y2K. Conversely, the more your economy is based on long-term relationships that do not easily change or adapt, the harder Y2K is likely going to be for you.

## Sharpen Your Scorer's Pencil



<b>More like U.S.</b>	<b>Less like U.S.</b>
<b>More rules, transparency</b>	<b>Fewer rules, less openness</b>
<b>More "New Economy"</b>	<b>Less "New Economy"</b>
<b>More wealthy, IT-savvy</b>	<b>Less wealthy, IT-savvy</b>
<b>Learned from 97-98 Crisis</b>	<b>Still learning from 97-98</b>

Slide 33: A Global Y2K Scorecard on 010100?

Wealthier states or firms will, in general, do better with Y2K due to the resources they can free up and bring to bear in terms of both remediation pre-010100 and consequence management post-010100. But even more important that resources is IT-savvy, since competency is the "long pole" in the tent, so some less wealthy states such as Ireland, a rising "virtual tiger economy" in its own right, should do well. On the other hand, poor and IT-backward economies are far more likely to be blind-sided by Y2K.

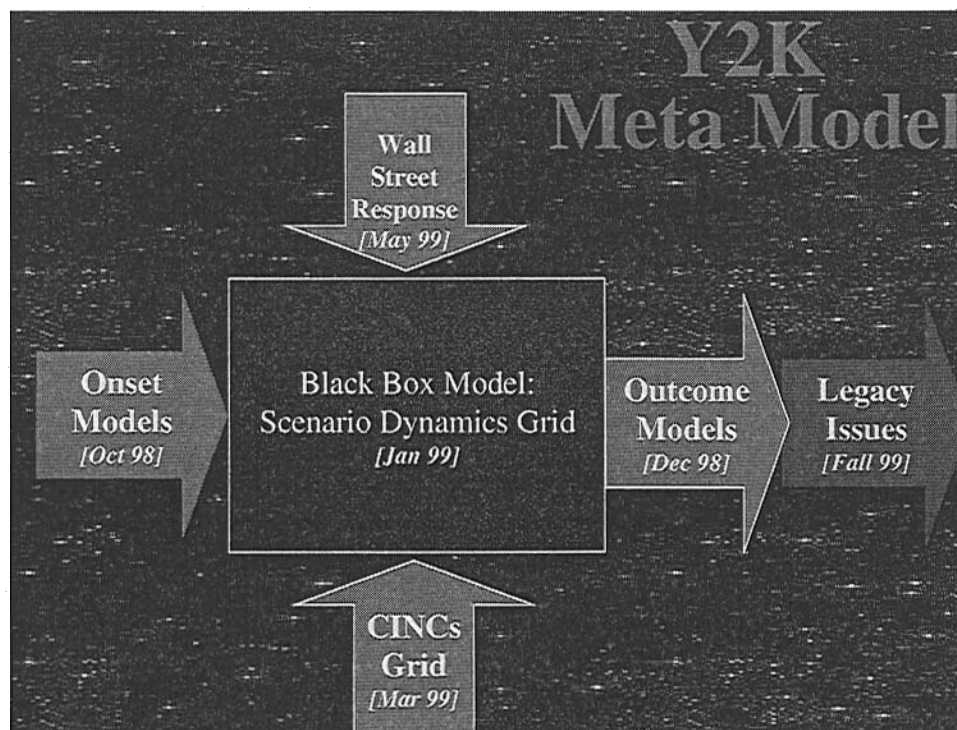
Finally, among the emerging economies (about 80 percent of the global population), those who have learned most and best from the 1997-1998 Global Financial Crisis (basically moving more in the direction of the previous four bullets above) will do far better than those who suffered much during the crisis and have done little to change. In short, Wall Street views the 1997-98 crisis as a wake-up call for having your house in order regarding Y2K in that the skill sets required to deal with each crisis are similar (i.e., the "basic fundamentals").

To sum up, there's not a lot of mystery, as far as Wall Street is concerned, regarding likely winners and losers with Y2K. Scorecards are already being prepared in global financial super-markets, and judgments are likely to be swift.

## VIII. Some Cosmic Conclusions About Y2K

### Our Y2K Meta Model: Connecting the Dots

While we won't pretend that we always knew where we were going with this project, it recently dawned on us that, in pursuing our various models and scenarios across our four workshops, we actually created what could be described as a Meta Y2K Model, i.e., a model of models. Slide 34 arrays our various models, grids, etc., in what we hope is a coherent pattern.



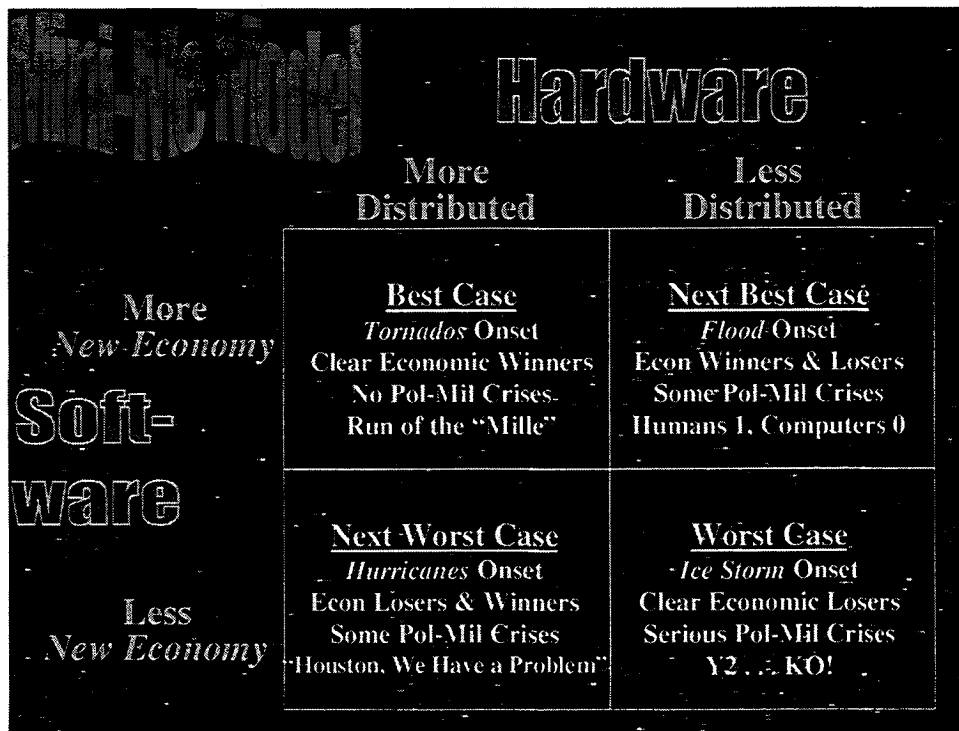
Slide 34: Year 2000 International Security Dimension Project "Meta Model" of Y2K

We explain the growth of this Meta Model as such:

- In October 1998 we developed our Onset Models (*Tornados, Flood, Hurricanes, Ice Storm*) to help us and others wrap their minds around the concept of what it would feel like when Y2K began to appear.
- In December 1998 we held our first workshop, the Scenario-Building Workshop, where our subject-matter experts helped us populate a series of generic Outcome Models (*Run of the "Mille"; Humans 1, Computers 0; Houston, We Have a Problem, Y2 KO!*). At that point, we felt we had a decent sense of some "going in" (Onset Models) and "coming out" (Outcome Models) scenarios, but very little sense of the dynamics in-between, i.e., the playing out of the Y2K Event itself.
- In January 1999 we held our second workshop, the Scenario-Dynamics Workshop, where our regional experts helped us populate a generic, composite, six-phase timeline Y2K Event scenario. The resulting framework, which we dubbed our Scenario Dynamics Grid, became our Black Box Model for explaining the range of possible dynamics that could be in play, in various combinations at various phases in the timeline, during any one country's Y2K Event experience.
- In March 1999 we held our third workshop, the Consequent Management Workshop, where our political-military experts helped us explore potential CINC strategies for dealing with Y2K-induced and related crises within individual theaters of operations around the world. In effect, we collectively examined how the U.S. Military could influence the playing out of the various scenario dynamics captured within our Black Box Y2K Model.
- In May 1999 we held our fourth and final workshop, the Economic Security Workshop, where our financial experts helped us explore how global markets would respond to and thus shape Y2K-induced or related economic crises around the world. Here we likewise collectively examined how Wall Street and other global super-markets could influence the playing out of the various scenario dynamics captured within our Black Box Y2K Model.
- Finally, what we plan to do in the fall of 1999 is hold one or more additional workshops with U.S. Government officials (namely, the U.S. Agency for International Development) to examine Y2K Legacy Models. Here we plan to explore *low probability, high impact* "wild cards" that may emerge from the Y2K Event.

## **Miniature Meta Model: We Call It . . . *Mini Me!***

Now, while we're happy that we can actually array all our models in a manner that seems to make some sense to us, we thought it made even more sense to try and distill that complex arrangement into something a bit more elegant. This Miniature Meta Model, or



Slide 35: Miniature "Meta Model" of Y2K, AKA *Mini Me*

what we like to call our "Mini Me" Model, boils down to two simple questions (presented in Slide 35):

- Hardware Question: How distributed is your country?
- Software Question: How "New Economy" is your economy?

Those two questions yield four outcome boxes, which, harkening back to our original X-Y axis, allows us to string together a series of individual judgments from our various models and workshops:

- *More New Economy + More Distributed = Best Case*
- *More New Economy + Less Distributed = Next Best Case*
- *Less New Economy + More Distributed = Next Worst Case*
- *Less New Economy + Less Distributed = Worst Case.*

Which countries go where? Well, we obviously see the U.S. and countries close to it in overall appearance and functioning to end up in the Best Case box. On the far extreme of that, we'd expect mono-political, mono-economic, mono-cultural, centralized states like an Iran or North Korea to be potential Worst Case situations, remembering our constant admonitions about asking the "So What?" question.

The in-between cases, of course, present the most intriguing situations.

A country like Japan or France could well end up in the Next Worst Case box as countries that are fairly distributed in terms of their networks, economies, etc., but are not yet adept at the playing the "New Economy" game that stresses rapidly shifting business relationships.

Most difficult to select are examples of countries that exhibit a lot of New Economy potential or capacity, but still have fairly centralized or collective economies married to unitary political states. These Next Best Case countries will inevitably be surprises, since they will be hit hard by Y2K, and yet seem to emerge stronger and more confident for the experience. In this light, one thinks of possibly South Korea or even China.

## **Conclusion #1—How You Describe Y2K Depends on From *When* You View It**

People who describe Y2K as "different in kind" from anything humanity has ever experienced, or something that is unique, tend to look at the event from the perspective of the past century. But those who look at Y2K from the perspective of the coming century, exhibit the exact opposite tendencies: they tend to describe Y2K as only "different in degree" from the sort of system perturbations humanity will increasingly face as we become more interconnected and interdependent on a global scale. In their minds, then, Y2K is a genuine harbinger of next definitions of international instabilities or uncertainty, in effect a new type of crisis that leaves us particularly uncomfortable with its lack of a clearly identifiable "enemy" or "threat" with associated motivations.

**Our bottom line (paraphrasing Rick in *Casablanca*): *We'll always have Y2K . . .***

## **Conclusion #2—Y2K Moves Us From *Haves-vs-Have Nots* to *Competents-vs-Incompetents***

Success at dealing with Y2K has a lot to do with resources, and anyone who believes otherwise is painfully naive. And yet, defeating the challenge of Y2K says as much or more about one's competency than it does about one's wealth. The rich can *survive* Y2K

just fine, but only the truly clever can *thrive* in Y2K, which IT competents tend to view as a sped-up market experience within the larger operational paradigm of the New Economy. The rise of "virtual tigers" such as India's software industry, Ireland's high-tech manufacturing, or Israel's Wadi Valley, tell us that it doesn't necessarily take a wealthy country to succeed in the New Economy, just a very competent one. Y2K may well serve as a microcosmic experience that drives this new reality home to many more around the planet: *it's less about what you have than what you can do*. For in the end, Y2K is less about vulnerability and dependency, then *dealing* with vulnerability and dependency. You can buy your way toward invulnerability and independence, but you can also *work around* vulnerabilities and dependency.

**Our bottom line:** *Competents will thrive, while incompetents nosedive.*

### **Conclusion #3—Y2K As A Glimpse Into the 21st Century: Divisions Become Less Vertical and More Horizontal**

The 20th Century featured an unprecedented amount of human suffering and death stemming from wars, and these conflicts came to embody humanity's definition of strife—namely, state-on-state warfare. The divisions that drove these conflicts can be described as "vertical," meaning peoples were separated—from top to bottom—by political and geographic boundaries, known as state borders.

If the 20th Century was the century of inter-state war, then the 21st is going to be the century of intra-state or civil strife. Divisions of note will exist on a "horizontal" plane, or between layers of people that coexist within a single state's population. These layers will be largely defined by wealth, as they have been throughout recorded history. But increasingly, that wealth will depend on competency rather than possession of resources.

Y2K will help crystallize this coming reality by demonstrating, in one simultaneous global experience, who is good at dealing with the New Economy, globalization, the Information Revolution, etc., and who is not. And these divisions will form more within countries than between them, as borders will become increasingly less relevant markers of where success begins and failure ends. The coming century of conflict will revolve around these horizontal divisions.

**Our bottom line:** *We have met the enemy, and they are us.*



## **Conclusion #4—Y2K Will Demonstrate the Price of Secrecy and the Promise of Transparency**

Those who are more open and transparent and share information more freely will do better with Y2K than those who hoard information, throw up firewalls, and refuse outside help. Secrecy will backfire in almost all instances, leading to misperceptions and harmful, stupidly self-fulfilling actions. Governments must be as open with their populations as possible, or suffer serious political backlashes if and when Y2K proves more significant for their countries than they had previously let on. People's fears about "invisible technology" will either be conquered or fed by how Y2K unfolds. This is a pivotal moment in human history: the first time Information Technology has threatened to bite back in a systematic way. In a very Nietzschean manner, Y2K will either "kill" us or make us stronger, and the balance of secrecy versus transparency will decide much, if not all, of that outcome.

**Our bottom line:** *The future is transparency—get used to it!*

## **Conclusion #5—Our Final Take on Y2K: As It Becomes Less Frightening, It Becomes More Profound**

The more you accept the notion that Y2K represents the future and not some accident of the past . . . the more you see it as different in degree than in kind from the challenges we will increasingly face . . . and the more you realize that it's part and parcel of the globalized, IT-driven New Economy than some exogenous one-time disaster, *then* the more profoundly will Y2K loom in your psyche even as it becomes less frightening with regard to the 010100-threshold. Why? Because the more it becomes associated with the broader reality of our increasingly interconnected and interdependent world, the more inescapable it becomes. In short, you can sit out the Millennium Date Change Event and all the hoopla surrounding it, but there's no avoiding Y2K in the big-picture sense, because the skills it demands from humanity are those same skills needed for our not-so-collective advance into the brave new world of the 21st Century.

**Our bottom line:** *There's no escaping Y2K.*

---

## **Appendix: List of Workshop Participants**

### **3-4 December 1998 Scenario-Building Workshop @ Decision Support Center, U.S. Naval War College, Newport RI**

The following individuals participated in the workshop:

- Wayne Bennett, lawyer, Bingham Dana LLP
- Suzanne Bergman, senior project engineer, Boeing
- Robert Bosnak, psychoanalyst, The Newport Institute
- Charles Cameron, fellow, The Arlington Institute
- Donald Clark, maritime data expert, I2 Technologies
- George Esper, journalist, Associated Press
- ADM William Flanagan, USN (ret), securities director, Cantor Fitzgerald LP
- Martin Gerra, management professor, College of Notre Dame of Maryland
- Philip Ginsberg, financial director, Cantor Fitzgerald LP
- Norm Green, deputy national intelligence officer for science & technology, National Intelligence Council
- Kent Harrington, media expert, The Harrington Group, LLC
- Michael Harrington, Y2K expert, MITRE Corporation
- Ethan Kapstein, professor of political economy, Univ. of Minnesota
- Paul Kourtz, technology expert, CIA
- Richard Landes, millennial history expert, Boston University
- Don Linford, banking official, Chase Manhattan

- Frank Mahncke, chief analyst, Dept. of Defense Joint Warfare Assessment Center
- Kenneth Malpass, telecommunications consultant, Stanford University
- Eugene Miasnikov, physicist, Moscow Institute of Physics and Technology
- Kathy Parker, social ecologist and long-time consultant to USAID
- Jeffrey Scannell, Y2K remediation expert and information technology consultant
- John Weiss, environmental affairs expert, CIA
- Nicholas Zvegintzov, software expert, Software Management Network.

## **13-15 January 1999 Scenario-Dynamics Workshop @ Clairborne Pell Center, Salve Regina University, Newport RI**

The following individuals participated in the workshop:

- Robert Bosnak, psychoanalyst, The Newport Institute
- Mark T. Dudman, director of software development, Comverse Network Systems
- Julia B. Gippenreiter, professor of psychology, Moscow State University
- Paula Gordon, visiting research professor, George Washington University
- Gabriel Gutierrez, economic consultant, UN Economic Commission for Latin America
- George Honadle, consultant, numerous international economic development agencies
- Michael Harrington (speaker), Y2K expert, MITRE Corporation
- Paul Kourtz, technology expert, CIA
- Richard Landes, millennial history expert, Boston University
- Jennifer Lee, Latin America specialist, Department of State

- Douglas MacIntyre, oil market analyst, Department of Energy
- Siphon Veli Mahlangu, risk analyst, National Year 2000 Decision Support Center of South Africa
- Angus McCrone, economic writer and consultant, Center for Economics and Business Research (UK)
- John Noer, project director, Center for Naval Analyses
- Kathy Parker, social ecologist and long-time consultant to USAID
- Daniel Pipes, editor, *Middle East Quarterly*
- Tony Pryor, Africa Bureau, U.S. Agency for International Development
- Jeffrey W. Schneider, South Asia specialist, Department of State
- Paul S. Triolo, Asian specialist, Department of State
- Mitzi Wertheim, senior manager, The CNA Corporation.

## **4 March 1999 Scenario-Strategies Workshop @ Center for Naval Analyses, The CNA Corporation, Alexandria VA**

The following individuals participated in the workshop:

- CDR Charles Adams, Y2K liaison, U.S. Coast Guard
- Ken Alnwick, Director of Gaming and Simulation Programs, Kapos Associates Inc.
- CAPT Joe Bouchard, staff member, National Security Council
- Jim Caverly, Office of Science and Technology Policy, Department of Energy
- VADM Arthur Cebrowski, President, U.S. Naval War College
- Ed Deagle, chairman, Potomac Finishing Company
- LTC Bill Finehout, J7 staff member, Joint Staff
- Jeff Gaynor, Director of Y2K Operations, OASD C3I

- CAPT Bill Gravell, staff member, CNO Executive Panel (N00K)
- Michael Harrington (speaker), Y2K expert, MITRE Corporation
- Paul Kourtz, technology expert, CIA
- Richard Landes, millennial history expert, Boston University
- Jennifer Lee, Latin America specialist, Department of State
- Maureen Lischke, administrator, U.S. Army National Guard
- Frank Mahncke, chief analyst, Dept. of Defense Joint Warfare Assessment Center
- Jim Melnick, J2 Y2K Working Group member, Joint Staff
- John Osterholz (presenter), Director of Information Integration and Interoperability, OASD C3I
- Daniel Pipes, editor, *Middle East Quarterly*
- RADM John Sigler, Director of Strategic Plans and Policy (J5), CENTCOM
- Olen Sisson, senior analyst, Department of Navy
- Paul S. Triolo, Asian specialist, Department of State
- Mitzi Wertheim, senior manager, The CNA Corporation
- Robert S. Wood, dean, U.S. Naval War College.

### **3 May 1999 Economic Security Workshop @ Cantor Fitzgerald LP, World Trade Center, New York NY**

The following individuals participated in the workshop:

- Bill Bone, Year 2000 administrator, NASD
- Dan Casey, IT administrator, Paribas
- Jim Caverly, Office of Science and Technology Policy, Department of Energy

- Len Costa, reporter, FORTUNE
  - ADM William Flanagan, USN (ret), securities director, Cantor Fitzgerald LP
  - Philip Ginsberg, financial director, Cantor Fitzgerald LP
  - Calvin Gooding, trader, Cantor Fitzgerald LP
  - Norm Green, deputy national intelligence officer for science & technology, National Intelligence Council
  - Damien Hart, chief trader, West Deuschelandes Bank
  - Kent Karosen, director, Cantor Fitzgerald LP
  - Glenn Kirwin, senior trader, Cantor Fitzgerald LP
  - Carolyn Landry, banking and finance analyst, National Intelligence Council
  - RADM Peter Long, Provost, U.S. Naval War College
  - Paul Nicholas, staff member, U.S. Senate Special Committee on the Year 2000 Technology Problem
  - Michael J. O'Connor, Y2K administrator, Merrill Lynch
  - John Rice, U.S. Treasurer, Citicorp Bank
  - William G. Roe, syndicate manager, Melhado, Flynn & Associates
  - CDR Gary Shrout, public affairs officer, U.S. Naval War College
  - Richard R. Snape, COO, Telerate
  - Robert Stevens, National Information Protection Center, FBI
  - Mitzi Wertheim, senior manager, The CNA Corporation
  - Robert S. Wood, dean, U.S. Naval War College.
-

CENTER FOR NAVAL WARFARE STUDIES

